JETROCK

User Manual

Configuration

First Edition, Sep 2008

korenix

www.korenix.com

Copyright Notice

Copyright© 2008 Korenix Technology Co., Ltd.
All rights reserved.
Reproduction without permission is prohibited.

Information provided in this manual is intended to be accurate and reliable. However, the original manufacturer assumes no responsibility for its use, or for any infringements upon the rights of third parties that may result from its use.
The material in this document is for product information only and is subject to change without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, Korenix assumes no liabilities resulting from errors or omissions in this document, or from the use of the information contained herein.
Korenix reserves the right to make changes in the product design without notice to its users.

Acknowledgments

Korenix is a registered trademark of Korenix Technology Co., Ltd.
All other trademarks or registered marks in the manual belong to their respective manufacturers.

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

The user is cautioned that changes and modifications made to the equipment without approval of the manufacturer could void the user's authority to operate this equipment.

Table of Contents

1. OVERVIEW 6

1.1. PRODUCT FEATURES 6
1.2. PACKAGE CHECKLIST 7
1.3. ABOUT THIS MANUAL 7

2. PREPARATION FOR MANAGEMENT 8

2.1. PREPARATION FOR CONSOLE MANAGEMENT 8
2.2. PREPARATION FOR NETWORK CONFIGURATION 8
2.3. PREPARATION FOR WEB MANAGEMENT 9
2.3.1. HTTP Web Interface 9
2.3.2. HTTPS Web Interface 10
2.4. PREPARATION FOR TELNET CONFIGURATION 11
2.4.1. Telnet 11
2.4.2. SSH (Secure Shell) 11

3. FEATURE CONFIGURATIONS 14

3.1. INTRODUCTION TO COMMAND LINE INTERFACE (CLI) 14
3.2. BASIC SETTINGS 18
3.2.1. Switch Setting 19
3.2.2. Admin Password 20
3.2.3. IP Configuration 20
3.2.4. Time Setting 21
3.2.5. DHCP Server and DHCP Option 82 Relay Agent 25
3.2.6. Backup and Restore 28
3.2.7. Firmware Upgrade 30
3.2.8. Factory Default 32
3.2.9. System Reboot 33
3.2.10. CLI Commands for Basic Settings 33
3.3. PORT CONFIGURATION 37
3.3.1. Port Control 38
3.3.2. Port Status 39
3.3.3. Rate Control 39
3.3.4. Command Lines for Port Configuration 40
3.4. NETWORK REDUNDANCY 42
3.4.1. RSTP 43

3.4.2. RSTP Information 46
3.4.3. Multiple Super Ring (MSR) 46
3.4.4. Ring Information 49
3.4.5. Command Lines for Network Redundancy 50
3.5. VLAN 54
3.5.1. Management VLAN 54
3.5.2. Port-Based VLAN Configuration 55
3.5.3. CLI Commands of the VLAN 56
3.6. Traffic Prioritization 57
3.6.1. QoS Setting 57
3.6.2. CoS-Queue Mapping 58
3.6.3. DSCP-Queue Mapping 59
3.6.4. CLI Commands for Traffic Prioritization 60
3.7. Multicast Filtering 63
3.7.1. IGMP Snooping 63
3.7.2. IGMP Query 64
3.7.3. CLI Commands of the Multicast Filtering 65
3.8. SNMP 66
3.8.1. SNMP Configuration 67
3.8.2. SNMP v3 Profile 67
3.8.3. SNMP Traps 68
3.8.4. CLI Commands for SNMP 69
3.9. Security 70
3.9.1. IP Security 70
3.9.2. CLI Commands for Security 71
3.10. Warning 71
3.10.1. Fault Relay Setting 72
3.10.2. Event Selection 74
3.10.3. SysLog Configuration 76
3.10.4. SMTP Configuration 76
3.10.5. CLI Commands for Warning 77
3.11. Monitoring and Diagnostic 80
3.11.1. MAC Address Table 80
3.11.2. Port Statistics 82
3.11.3. Event Log 83
3.11.4. Ping Utility 83
3.11.5. CLI Commands for Monitoring and Diagnostic 84
3.12. Device Front Panel 86

3.13. SAVE TO FLASH 86
3.13.1. CLI Commands for Save to Flash 87
3.14. LOGOUT 87
3.14.1. CLI Commands for Logout 87
APPENDIX A. KORENIX PRIVATE MIB 88
APPENDIX B. TECHNICAL DATA 89
B.1. JETNET 4506-RJ 89
B.2. JETNET 4506-M12 91
B.3. JETNET 3006-RJ 93
B.4. JETNET 3006-M12 94
B.5. JETNET 3706-RJ 95
FURTHER SUPPORT 97

1. Overview

JetRock series is designed to provide ultra rugged and long-life protection against the roughest industrial usage without the need of additional shelters. The totally sealed enclosure achieves the highest level of protection, IP67 and IP68. JetRock Series is equipped with rugged RJ45 and M12 connectors for a secured, robust connection under the most brutal environments.

With the highest grade of protection, JetRock series can be used in various locations and applications. From automation and plant floor, to offshore and pharmaceutical, the JetRock is the perfect fit many tough industrial needs.

1.1. Product Features

JetRock models have the following features:

- IP67 / IP68 enclosure protection
- Robust connection against shock and vibration
- Store and forward switch technology
- Broadcast storm filtering
- 2K MAC address table
- Transfer packet size from 64 to 1536 bytes
- JetNet 3706-RJ is IEEE 802.3af PoE enabled.

The managed models, JetNet 4506-RJ and JetNet 4506-M12, provide a large range of functions:

- Korenix patented redundant ring technology, Rapid Super Ring
- RSTP redundancy
- Port-based VLAN
- IGMP Snooping and Query
- DHCP server, client and relay agent for DHCP option 82
- IP security against unauthorized access
- Traffic priority
- Rate control and flow control
- NTP for system time synchronization
- Alarm relay for events of ring failure, link down, and power failure
- SNMP
- Web-based interface
- Command Line Interface – CLI

1.2. Package Checklist

JetRock is shipped with the following items. If any of these items is missing or damaged, please contact your customer service representative for assistance.

	JetNet 4506-RJ	JetNet 4506-M12	JetNet 3006-RJ	JetNet 3006-M12	JetNet 3706-RJ
• JetRock Unit	1	1	1	1	1
• M12 A-coding 5-pole Female Field Assembleable Connecter	1	1	1	1	1
• M12 on RJ45 Ethernet Cable		1			
• M12 on DB9 Shielded Console Cable	1	1			
• Rugged RJ45 Field Assembleable Connecter	6		6		6
• Wall-Mount Screws, Washer and Nuts	4	4	4	4	4
• 1:1 Wall-Mount Drilling Template	1	1	1	1	1
• Quick Installation Guide	1	1	1	1	1
• Documentation and Software CD-ROM	1	1	1	1	1

1.3. About This Manual

The following manuals are included as PDF files on the CD-ROM:

- User manual – Hardware Installation: includes information to install all versions of JetRock products, JetNet 4506-RJ, JetNet 4506-M12, JetNet 3006-RJ, JetNet 3006-M12, and JetNet 3706-RJ.
- User manual – Configuration: apply to the managed versions of JetRock, which are JetNet 4506-RJ, JetNet 4506-M12.

2. Preparation for Management

JetRock provides both in-band and out-band configurations. With out-band management, you can configure the switch via RS232 console if you do not want to include your admin PC as part of your network. In case of losing network connection, you still need the ability to configure the switch via RS232 console. Out-band management does not affect network performance.

In-band management allows you remotely manage the switch through the network, either by Telnet or by Web. You just need the device's IP address to connect to its Telnet console and its embedded HTTP web pages.

2.1. Preparation for Console Management

Connect to the device by the M12 on DB9 console cable

1. Go to Start→Program→Accessories→Communication→Hyper Terminal
2. Give a name to the new console connection
3. Choose the COM name
4. Select correct serial settings. The serial settings for the JetRock are: Baud Rate: 9600 / Parity Check: None / Data Bit: 8 / Stop Bit: 1
5. After connected, you will see a login request. The default username and password is **admin/admin**

```
Booting...
Switch login: admin
Password:

JetNet 4506-M12 (version 2.1-20080909).
Copyright 2006-2008 Korenix Technology Co., Ltd.
Switch>
```

2.2. Preparation for Network Configuration

Before managing the device through telnet or web connection, please verify the device is installed properly on your network.

1. Make sure the network interface card (NIC) of your computer is working and

its operating system supports TCP/IP protocol.

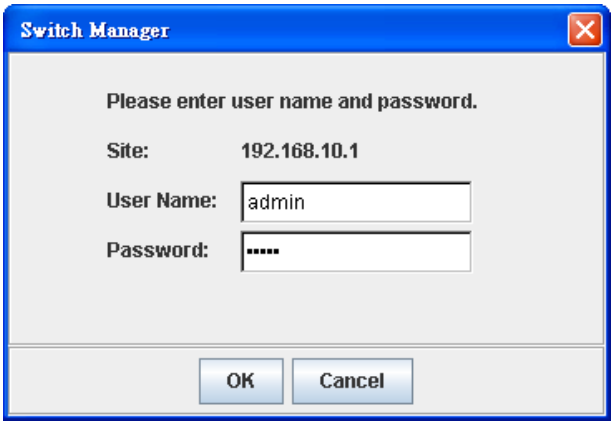
2. Turn on the switch and connect the switch to your computer.
3. Make sure the device is properly connected to your local network, and its IP configuration is on the same subnet. Simply use JetView to discover the device and change its IP address.
4. Use the DOS command "ping" to verify if the network connection between the switch and your computer is working correctly.

2.3. Preparation for Web Management

JetRock provides both HTTP Web interface and Secure HTTPS Web interface for management. The web page uses JavaScript which allows you to use a standard web browser such as Microsoft Internet Explorer or Mozilla FireFox to configure the switch from anywhere while connected to the network.

2.3.1. HTTP Web Interface

1. Launch web browser.
2. Connect URL of the device. The URL of the device is its IP address, for example http://192.168.10.1 for the default IP address or the IP address you assigned to it.
3. Login user name and password. The default username and password is **admin/admin**.



Click **OK**. The welcome page of the web-based management interface will now appear.

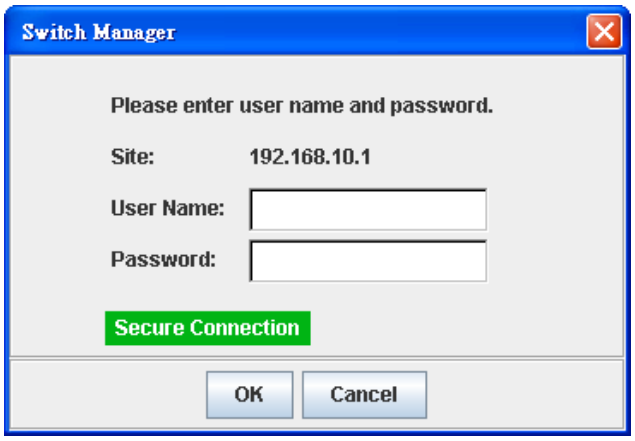
Note: Internet Explorer Version 5.0 or later does not allow Java applets to open sockets by default. Users must directly modify the browser settings to selectively enable Java applets in order to use network ports.

Note: The management session will timeout automatically if you do not input anything after 30 seconds. Re-login if this occurs.

2.3.2. HTTPS Web Interface

HTTPS provides secure network connection. The username, password, and all the commands and responses are encrypted against peeping.

1. Launch web browser.
2. Connect URL of the device. The URL of the device is its IP address, for example https://192.168.10.1 for the default IP address or the IP address you assigned to it.
3. A window will popup and ask you to trust the secure HTTPS session. Press Yes.
4. Login user name and password. The default username and password is **admin/admin**.



2.4. Preparation for Telnet Configuration

2.4.1. Telnet

The command of Telnet management is the same as the command of console. Follow the below steps for starting a Telnet session:

1. Go to Start -> Run -> cmd. Press **Enter**
2. Type "Telnet 192.168.10.1" (or the IP address of the switch). Press **Enter**

2.4.2. SSH (Secure Shell)

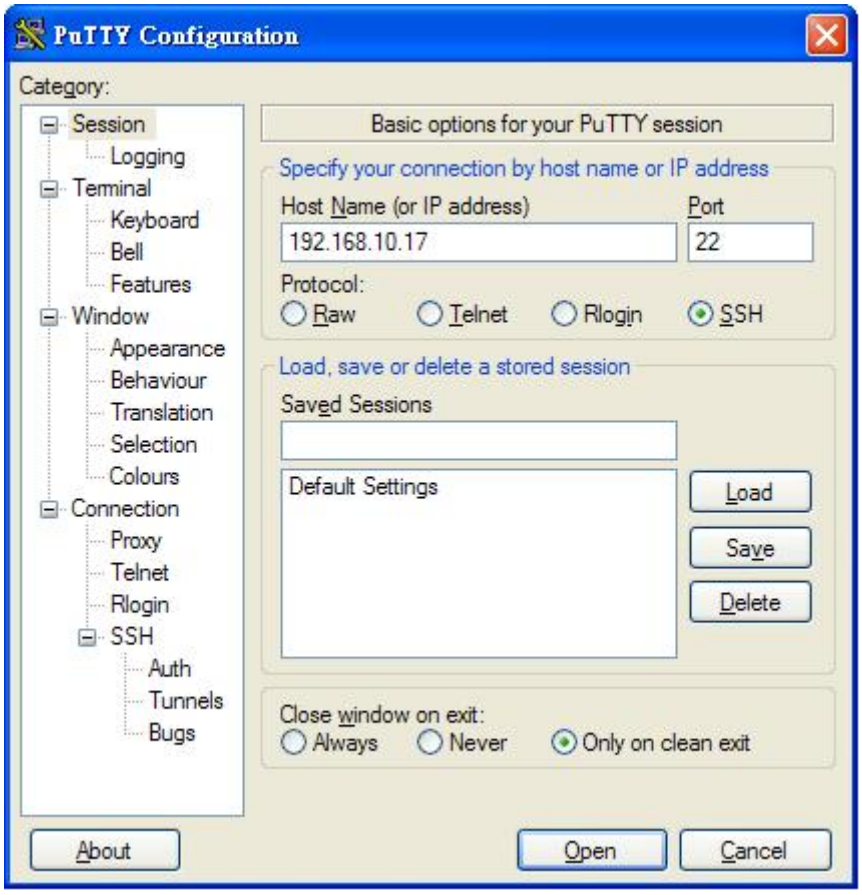
SSH, which provides a secure command line interface, operates in client/server architecture. While the device acts as the SSH server, you need a SSH client application before making a SSH connection to the switch.

There are many SSH clients you can find on the internet, such as *PuTTY*. We take PuTTY as an example to describe how to use SSH.

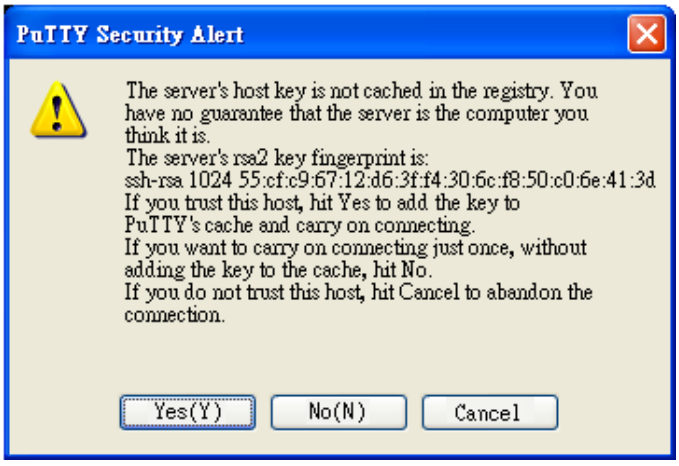
Note: PuTTY, Copyright 1997-2006 Simon Tatham.

Download PuTTY: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

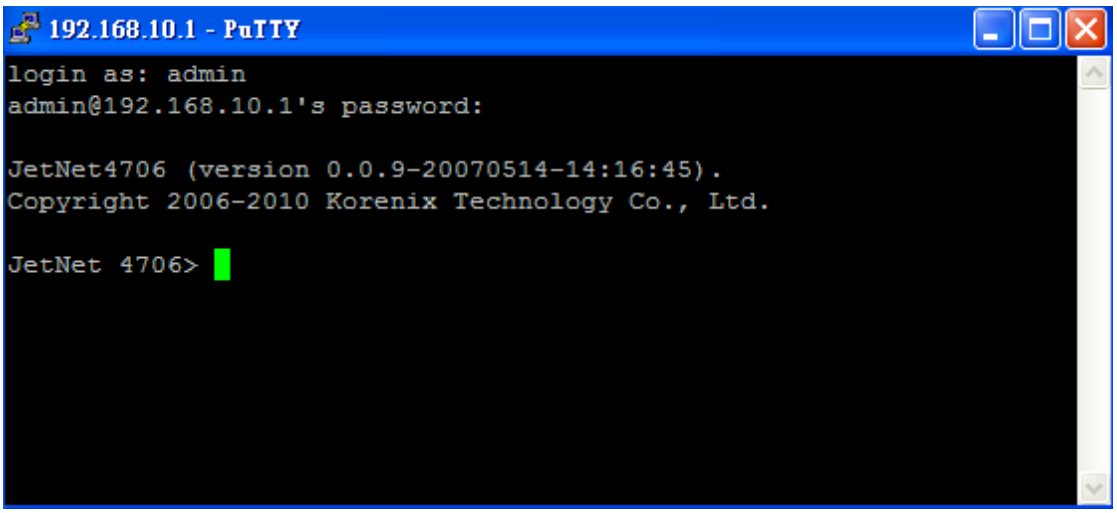
1. Launch SSH Client (PuTTY): In the **Session** configuration, enter the **Host Name** (the IP Address of the switch) and **Port number** (default = 22). Choose "**SSH**" protocol. Click "**Open**" to start a SSH session.



2. After clicking **Open**, you will see the cipher information in the popup screen. Press **Yes** to accept the Security Alert.


PuTTY Security Alert
The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 1024 55:cf:c9:67:12:d6:3f:f4:30:6c:f8:50:c0:6e:41:3d
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.
Yes(Y)
No(N)
Cancel

3. After a few seconds, the SSH connection opens.



4. The default login name and password is **admin/admin.**
5. All the commands you see in SSH are the same as the commands you see via console. The next chapter will introduce in detail how to use the command line to configure the switch

3. Feature Configurations

3.1. Introduction to Command Line Interface (CLI)

The Command Line Interface (CLI) is the user interface of the switch's embedded software system. You can view the system information, see the status, configure the switch and receive a response back from the system by keying in a command.

There are different command modes. Each command mode has its own access ability, its own available command lines, and its own different command lines to enter and exit. These modes are **User EXEC, Privileged EXEC, Global Configuration,** and **(Port/VLAN) Interface Configuration modes**.

User EXEC mode: As long as you login to the switch through CLI, you will be in the User EXEC mode. You can ping, telnet remote device, and show some basic information.

```
Switch>
  enable          Turn on privileged mode command
  exit            Exit current mode and down to previous mode
  list            Print command list
  ping            Send echo messages
  quit            Exit current mode and down to previous mode
  show            Show running system information
  telnet          Open a telnet connection
  traceroute      Trace route to destination
```

Types **enable** to enter the next mode, and **exit** to logout. Below is a full command list.

Privileged EXEC mode: Type **enable** in the User EXEC mode to enter the Privileged EXEC mode. In this mode, the system allows you to view current configurations, reset to default, reload the switch, show the system's information, save a configuration, and enter the global configuration mode.

You can type **configure terminal** to enter the next mode or **exit** to leave, to see a list of available command by types **?**. Following diagram shows the commands.

```
Switch(config)# ?
  access-list         Add an access list entry
  administrator       Administrator account setting
  arp                 Set a static ARP entry
  clock               Configure time-of-day clock
  default             Set a command to its defaults
  end                 End current mode and change to enable mode
  exit                Exit current mode and down to previous mode
  hostname            Set system's network name
  interface           Select an interface to configure
  ip                  IP information
  list                Print command list
  log                 Logging control
  mac                 Global MAC configuration subcommands
  mac-address-table   mac address table
  no                  Negate a command or set its defaults
  ntp                 Configure NTP
  password            Assign the terminal connection password
  qos                 Quality of Service (QoS)
  relay               relay output type information
  rmon                Remote monitoring
  router              Enable a routing process
  smtp-server         SMTP server configuration
  snmp-server         the SNMP server
  spanning-tree       the spanning tree algorithm
  super-ring          the super-ring protocol
  warning-event       Warning event selection
  write-config        Specify config files to write to
Switch(config)#
```

Global Configuration mode: Type **configure terminal** in privileged EXEC mode. You can then enter the global configuration mode. In global configuration mode, you can configure all the features that the system provides.

Type **interface IFNAME/VLAN** to enter interface configuration mode and **exit** to leave, or **?** for command list.

(Port) Interface Configuration: Type **interface IFNAME** in global configuration mode. You can then enter interface configuration mode. In this mode, you can configure port settings.

The port interface name for fast Ethernet port 1 is fa1; fast Ethernet 6 is fa6. You can type the interface name accordingly when you want to enter a specific interface configuration mode.

You can type **exit** to leave or **"?"** for a list of available commands.

Below are the available commands for port interface configuration mode.

```
Switch(config)# interface fa2
Switch(config-if)#
  auto-negotiation  Enables auto-negotiation state of a given port
  description       Interface specific description
  duplex            Specifies the duplex mode of operation for a port
  end               End current mode and change to enable mode
  exit              Exit current mode and down to previous mode
  flowcontrol       Sets the flow-control value for an interface
  list              Print command list
  loopback          Specifies the loopback mode of operation for a port
  mac               MAC interface commands
  mdix              Enables mdix state of a given port
  no                Negate a command or set its defaults
  poe               Configure power over ethernet
  qos               Quality of Service (QoS)
  quit              Exit current mode and down to previous mode
  rate-limit        Rate limit configuration
  shutdown          Shutdown the selected interface
  spanning-tree     the spanning-tree protocol
  speed             Specifies the speed of a Fast Ethernet port.
  switchport        Set switching mode characteristics
```

(VLAN) Interface Configuration: Type **interface VLAN VLAN-ID** in global configuration mode. You can then enter the VLAN interface configuration mode. In this mode, you can configure the settings for a specific VLAN.

The VLAN interface name for VLAN 1 is VLAN 1; VLAN 2 is VLAN 2.

You can type **exit** to leave or "**?** " for a list of available commands.

Available commands for the VLAN interface configuration mode appear below.

```
Switch(config)# interface vlan 1
switch(config-if)#
  Description   Interface specific description
  end           End current mode and change to enable mode
  exit          Exit current mode and down to previous mode
  ip            Interface Internet Protocol config commands
  list          Print command list
  no            Negate a command or set its defaults
  quit          Exit current mode and down to previous mode
  shutdown      Shutdown the selected interface
```

The following is a summary of command modes.

Command Mode	Main Function	Enter and Exit Method	Prompt
User EXEC	This is the first level of access. Users can ping, telnet remote device, and show basic information	Enter: **Type login** to login Exit: Type **exit** to logout Next mode: Type **enable** to enter privileged EXEC mode.	Switch>

Privileged EXEC	In this mode, the system allows you to view current configuration, reset to default, reload the switch, show the system's information, save a configuration, and enter global configuration mode.	Enter: Type **enable** in User EXEC mode. Exec: Type **disable** to exit to user EXEC mode. Type **exit** to logout Next Mode: Type **configure terminal** to enter global configuration command.	Switch#
Global configuration	In global configuration mode, you can configure all the features that the system provides	Enter: Type **configure terminal** in privileged EXEC mode Exit: Type **exit** or **end** or press **Ctrl-Z** to exit. Next mode: Type **interface IFNAME/ VLAN VID** to enter interface configuration mode	Switch(config)#
Port Interface configuration	In this mode, you can configure port-related settings.	Enter: Type **interface IFNAME** in global configuration mode. Exit: Type **exit** or **Ctrl+Z** to global configuration mode. Type **end** to privileged EXEC mode.	Switch(config-if)#
VLAN Interface Configuration	In this mode, you can configure settings for specific VLAN.	Enter: Type **interface VLAN VID** in global configuration mode. Exit: Type **exit** or **Ctrl+Z** to global configuration mode. Type **end** to privileged EXEC mode.	Switch(config-vlan)#

Here are some useful commands for you to see all or specific commands available to you. Save time and avoid typing errors.

? Shows all the available commands in the mode you are currently in. It also shows you the next command you can/should type.

```
Switch(config)# interface (?)
  IFNAME        Interface's name
  vlan          Select a vlan to configure
```

(Character)? Shows all the available commands for what you input as "Character."

```
Switch(config)# a?
  access-list        Add an access list entry
  administrator      Administrator account setting
  arp                Set a static ARP entry
```

Tab Key Helps you input commands quicker. If there is only one available command, hitting the tab key can help you automatically generate the command.

```
Switch# co (tab) (tab)
Switch# configure terminal

Switch(config)# ac (tab)
Switch(config)# access-list
```

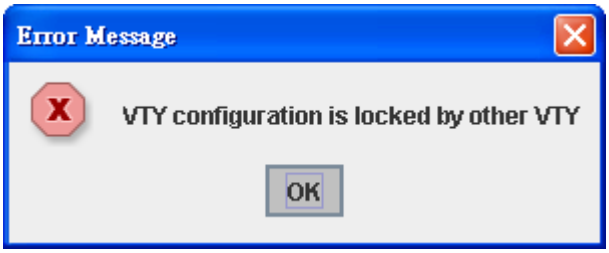
Ctrl+C Stops an unfinished command.

Ctrl+S Locks the screen of the terminal. You will not be able to input a command.

Ctrl+Q Unlocks a locked screen.

Ctrl+Z Exits configuration mode.

An alert message appears when multiple users try to configure the switch. If the administrator is in configuration mode, then Web users will not be able to change the settings. Only one administrator is allowed to configure the switch at a time.



3.2. Basic Settings

This section provides you with instructions on how to configure switch information, set the IP address, and configure the username and password of the system. It also allows you to upgrade the firmware, backup and restore a configuration, reload the system to factory default, and reboot the system.

3.2.1. Switch Setting

You can assign a System name, Location, Contact and view the system information. The following figure is the Web UI for Switch Setting.

System Name Assign a name to the device. You can input up to 64 characters. After you configure the name, the CLIP system will select the first 12 characters as the name for the CLIP system.

System Location Specify the switch's physical location. You can input up to 64 characters.

System Contact Specify contact people. Enter the name, e-mail address or other information about the administrator. You can input up to 64 characters.

System OID Set the SNMP object ID of the switch. You can follow the path to find its private MIB in the MIB browser. **Note:** When you attempt to view a private MIB, you should compile private MIB files into your MIB browser first.

System Description View a description of the system.

Firmware Version Display the firmware version installed on this device.

Device MAC Display the unique hardware address (MAC address)

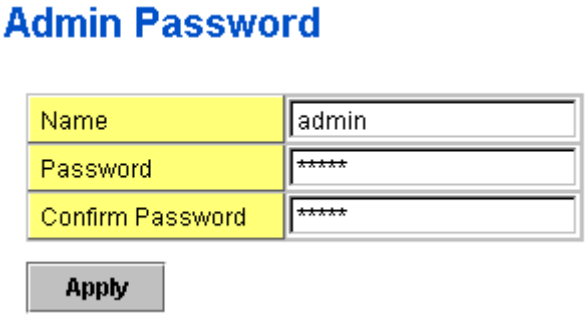
assigned by the manufacturer.

Once you have finished the configuration, click the **Apply** button to apply your settings.

Note: Always remember to select **Save** to save your settings. Otherwise, the settings you made will be lost when the switch is powered off.

3.2.2. Admin Password

You can change the username and password to enhance security. The following figure is the Web UI for Admin Password



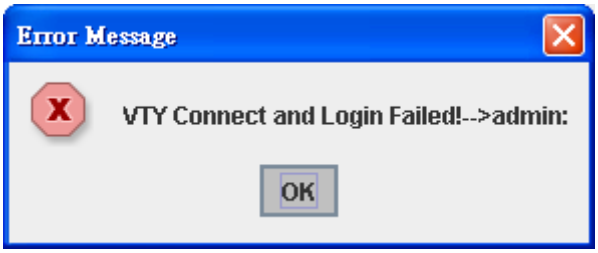
Username Key in a new username. The default setting is **admin**

Password Key in a new password. The default setting is **admin**

Confirm Password Re-enter the new password to confirm it

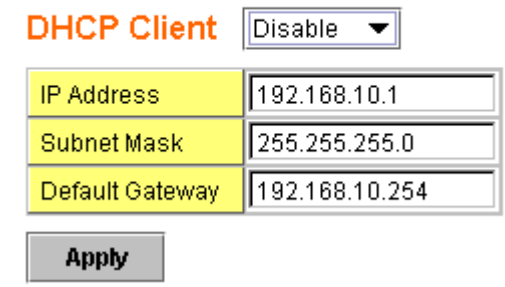
Once you finish configuring the settings, click the **Apply** button to apply your configuration.

The following figure is the popup alert window when the incorrect username is entered.



3.2.3. IP Configuration

This function allows users to configure the switch's IP address settings.



DHCP Client Enable or Disable DHCP Client function. When DHCP Client function is enabled, an IP address will be assigned to the switch from a network's DHCP server. In this mode, the default IP address will be replaced by the one assigned by the DHCP server. If DHCP Client is disabled, then the IP address that you specified will be used instead.

IP Address Assign an IP address for the device. If DHCP Client function is enabled, you don't need to assign an IP address, as it will be overwritten by the DHCP server. The default IP address is 192.168.10.1.

Subnet Mask Assign the subnet mask for the IP address. If DHCP Client function is enabled, you don't need to assign the subnet mask. The default Subnet Mask is 255.255.255.0.

Note: In the CLI, we use the enabled subnet mask to represent the number displayed in the web UI. For example, 8 stands for 255.0.0.0; 16 stands for 255.255.0.0; 24 stands for 255.255.255.0.

Gateway Assign the gateway for the switch. The default gateway is 192.168.10.254.

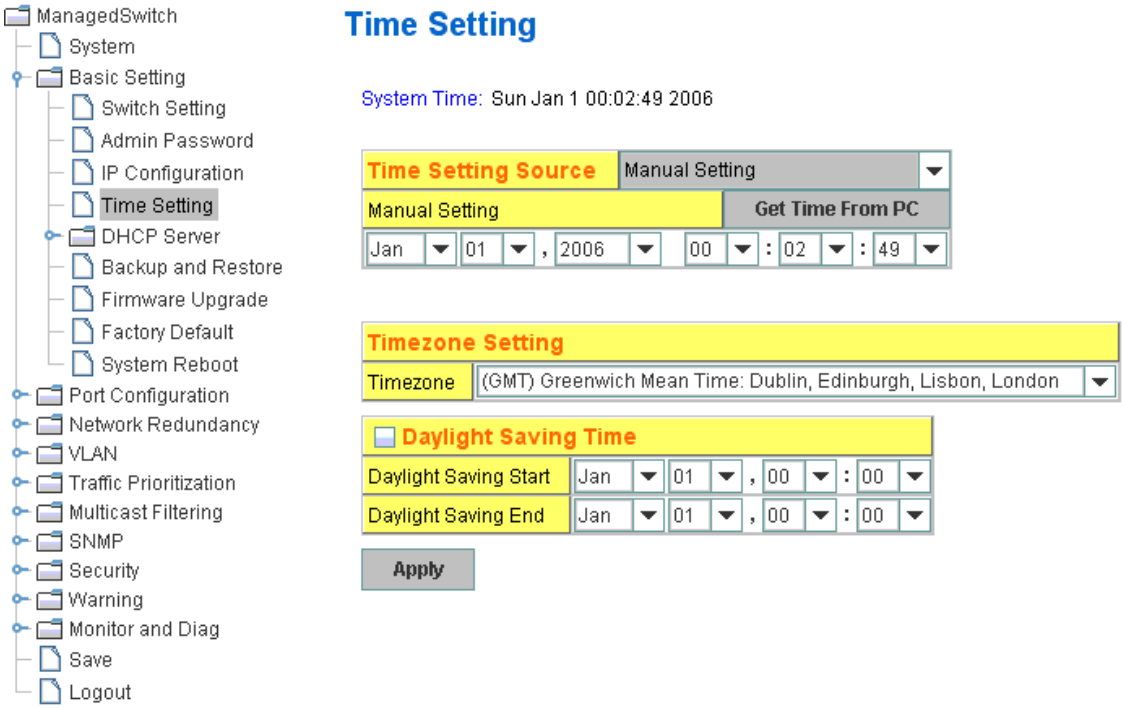
Note: In the CLI, we use 0.0.0.0/0 to represent the default gateway.

Once you finish configuring the settings, click the **Apply** button to apply your configuration.

3.2.4. Time Setting

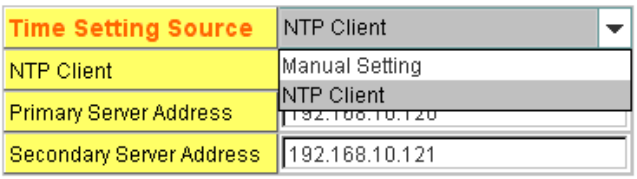
Time Setting source allow user to set the time by manually or through NTP server. It also provide time synchronize from PC. Network Time Protocol (NTP) is used to synchronize computer clocks on the internet. You can configure NTP settings

here to synchronize the clocks of several switches on the network. Daylight Saving Time function is also provided.



Manual Setting User can select Manual setting to change time as user want and also click the icon "Get Time From PC" to sync time from your PC.

NTP client Select the Time Setting Source to NTP client can let device enable the NTP client.It allow the switch get time from 2 different NTP servers. The system will send request packet to acquire current time from the NTP server.



Time zone Select the time zone where the switch is located. For your reference, the following table lists the time zones of different locations. The default time zone is GMT (Greenwich Mean Time).

```
Switch(config)# clock timezone
  01  (GMT-12:00) Eniwetok, Kwajalein
  02  (GMT-11:00) Midway Island, Samoa
  03  (GMT-10:00) Hawaii
```

04 (GMT-09:00) Alaska
05 (GMT-08:00) Pacific Time (US & Canada) , Tijuana
06 (GMT-07:00) Arizona
07 (GMT-07:00) Mountain Time (US & Canada)
08 (GMT-06:00) Central America
09 (GMT-06:00) Central Time (US & Canada)
10 (GMT-06:00) Mexico City
11 (GMT-06:00) Saskatchewan
12 (GMT-05:00) Bogota, Lima, Quito
13 (GMT-05:00) Eastern Time (US & Canada)
14 (GMT-05:00) Indiana (East)
15 (GMT-04:00) Atlantic Time (Canada)
16 (GMT-04:00) Caracas, La Paz
17 (GMT-04:00) Santiago
18 (GMT-03:00) NewFoundland
19 (GMT-03:00) Brasilia
20 (GMT-03:00) Buenos Aires, Georgetown
21 (GMT-03:00) Greenland
22 (GMT-02:00) Mid-Atlantic
23 (GMT-01:00) Azores
24 (GMT-01:00) Cape Verde Is.
25 (GMT) Casablanca, Monrovia
26 (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
27 (GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
28 (GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
29 (GMT+01:00) Brussels, Copenhagen, Madrid, Paris
30 (GMT+01:00) Sarajevo, Skopje, Sofija, Vilnius, Warsaw, Zagreb
31 (GMT+01:00) West Central Africa
32 (GMT+02:00) Athens, Istanbul, Minsk
33 (GMT+02:00) Bucharest
34 (GMT+02:00) Cairo
35 (GMT+02:00) Harare, Pretoria
36 (GMT+02:00) Helsinki, Riga, Tallinn
37 (GMT+02:00) Jerusalem
38 (GMT+03:00) Baghdad
39 (GMT+03:00) Kuwait, Riyadh
40 (GMT+03:00) Moscow, St. Petersburg, Volgograd
41 (GMT+03:00) Nairobi

42 (GMT+03:30) Tehran
43 (GMT+04:00) Abu Dhabi, Muscat
44 (GMT+04:00) Baku, Tbilisi, Yerevan
45 (GMT+04:30) Kabul
46 (GMT+05:00) Ekaterinburg
47 (GMT+05:00) Islamabad, Karachi, Tashkent
48 (GMT+05:30) Calcutta, Chennai, Mumbai, New Delhi
49 (GMT+05:45) Kathmandu
50 (GMT+06:00) Almaty, Novosibirsk
51 (GMT+06:00) Astana, Dhaka
52 (GMT+06:00) Sri Jayawardenepura
53 (GMT+06:30) Rangoon
54 (GMT+07:00) Bangkok, Hanoi, Jakarta
55 (GMT+07:00) Krasnoyarsk
56 (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi
57 (GMT+08:00) Irkutsk, Ulaan Bataar
58 (GMT+08:00) Kuala Lumpur, Singapore
59 (GMT+08:00) Perth
60 (GMT+08:00) Taipei
61 (GMT+09:00) Osaka, Sapporo, Tokyo
62 (GMT+09:00) Seoul
63 (GMT+09:00) Yakutsk
64 (GMT+09:30) Adelaide
65 (GMT+09:30) Darwin
66 (GMT+10:00) Brisbane
67 (GMT+10:00) Canberra, Melbourne, Sydney
68 (GMT+10:00) Guam, Port Moresby
69 (GMT+10:00) Hobart
70 (GMT+10:00) Vladivostok
71 (GMT+11:00) Magadan, Solomon Is., New Caledonia
72 (GMT+12:00) Aukland, Wellington
73 (GMT+12:00) Fiji, Kamchatka, Marshall Is.
74 (GMT+13:00) Nuku'alofa

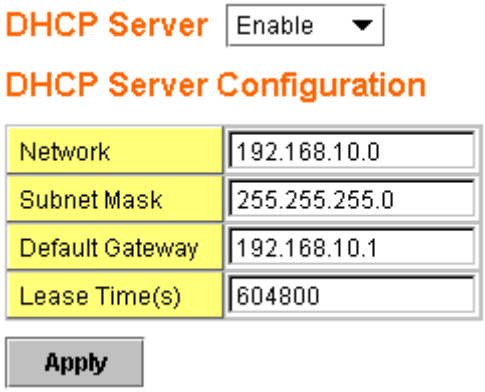
Daylight Saving Time Set when Enable Daylight Saving Time start and end, During the Daylight Saving Time, the device's time is one hour earlier than the actual time.

Once you have finished the configuration, click the **Apply** button to apply your configuration.

3.2.5. DHCP Server and DHCP Option 82 Relay Agent

Dynamic Host Configuration Protocol (DHCP) is a protocol used by networked devices (clients) to obtain the parameters necessary for operation in an IP network. The protocol works in a client/server model. The server automates the assignment of IP addresses, subnet masks, default gateway, and other IP parameters to the client.

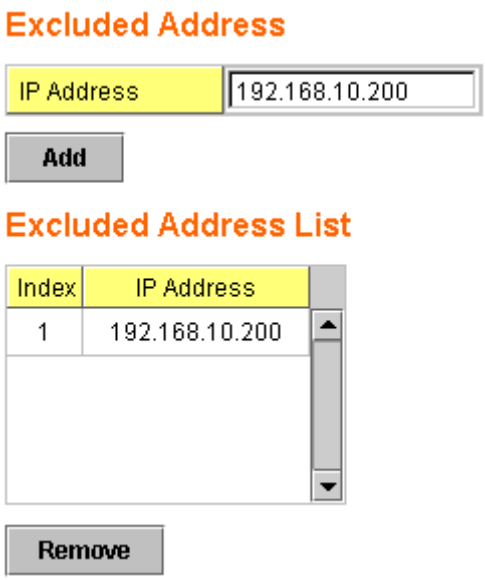
This switch can act as a DHCP server which helps to reduce system administration workload, allowing devices to be added to the network with little or no manual configuration.



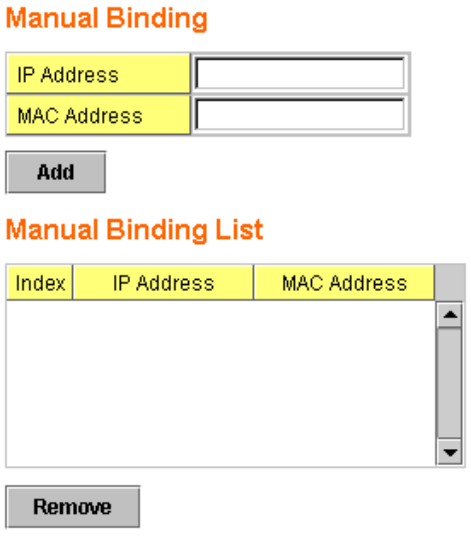
DHCP Server — Enable or Disable DHCP Server function. A switch acts as a DHCP server will assign a new IP address to link partners.

DHCP Server configuration — After selecting to enable DHCP Server function, type in the Network IP address for the DHCP server IP pool, Subnet Mask, Default Gateway address and Lease Time for client.

Once you have finished the configuration, click the **Apply** button to apply your configuration.

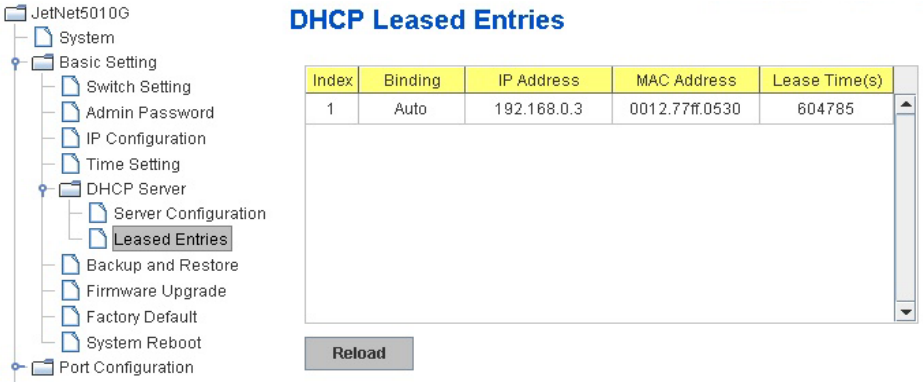


Excluded Address You can type a specific address into the **IP Address field** for the DHCP server reserved IP address. The IP address that is listed in the **Excluded Address List Table** will not be assigned to the network device. Add or remove an IP address from the **Excluded Address List** by clicking the **Add** or **Remove** button.



Manual Binding The binding between a MAC address and an IP address can be fixed. You can type in the specified IP and MAC address, and then click the **Add** button to add a new MAC&IP address binding rule for a specified link partner, like PLC or any device without **DHCP client** function. To remove from the binding list, just select the rule to remove and click the **Remove** button.

Once you have finished the configuration, click the **Apply** button to apply your configuration.

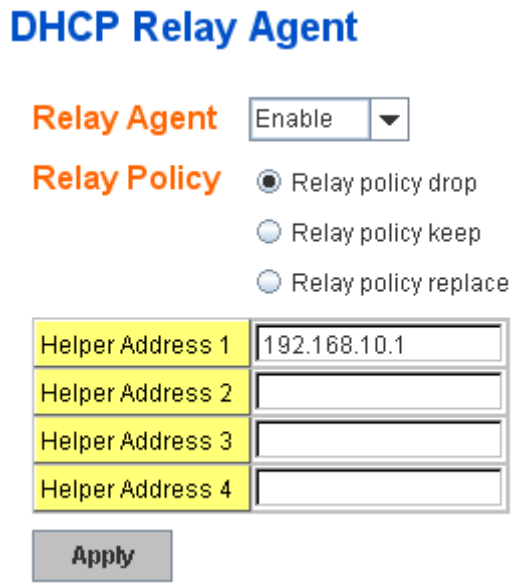


DHCP Leased Entries A table shows the MAC and IP address that was currently assigned by this switch. Click the **Reload** button to refresh the listing.

DHCP Option 82 Relay Agent

The DHCP relay agent information option (option 82) enables a DHCP relay agent to include information about itself when forwarding client-originated DHCP packets to a DHCP server. The DHCP server can use this information to implement IP address or other parameter-assignment policies. This feature gives you the option of always assigning the same IP address to any device which is connected to a particular location (port of a device) on the LAN.

This switch is able to be a DHCP relay agent.



Relay Agent Enable/disable relay agent

Relay Policy Set the relay policy for receiving a DHCP packet that has an option 82 field.

	Relay Policy Drop	drops the option 82 field and do not add any other option 82 field.
	Relay Policy Keep	keeps the original option 82 field and forwards to server.
	Relay Policy Replace	replaces the existing option 82 field and adds new option 82 field. This is the default setting.
Helper Address	Specify the IP address of DHCP Server that Relay Agent forwards to. There are 4 IP setting at most.	

Once you have finished the configuration, click the **Apply** button to apply your configuration.

3.2.6. Backup and Restore

With the Backup command, you can save current configuration files saved in the switch's flash to the admin PC or TFTP server. This will allow you to restore the configuration file back to the switch. Before you restore the configuration file, you must place the backup configuration file into the PC or TFTP server. The switch will then download this file back to the flash.

There are 2 modes to backup/restore the configuration file, Local File mode and TFTP Server mode.

Local File mode: In this mode, the switch acts as the file server. User browses the target folder and gives a file name to backup the configuration. User can also browse the target folder and select existing configuration files to restore the configuration back to the switch. This mode is only provided by Web UI. CLI is not supported.

TFTP Server mode: In this mode, the switch acts as TFTP client. Make sure your TFTP server is ready. Enter the IP address of the TFTP Server. The system uses the default configuration file name, **Quagga.conf.** You do not need to enter a new file name. This mode is supported in both Web UI and CLI.

TFTP Server IP Address: Key in the IP address of your TFTP Server here.

Backup/Restore File Name: The system uses a default file name.

Configuration File: The configuration file of the switch is a text file. You can open it with *Microsoft Word* or any program that can read .txt files, modify the file, add/remove configuration settings, and then restore it back on to the switch.

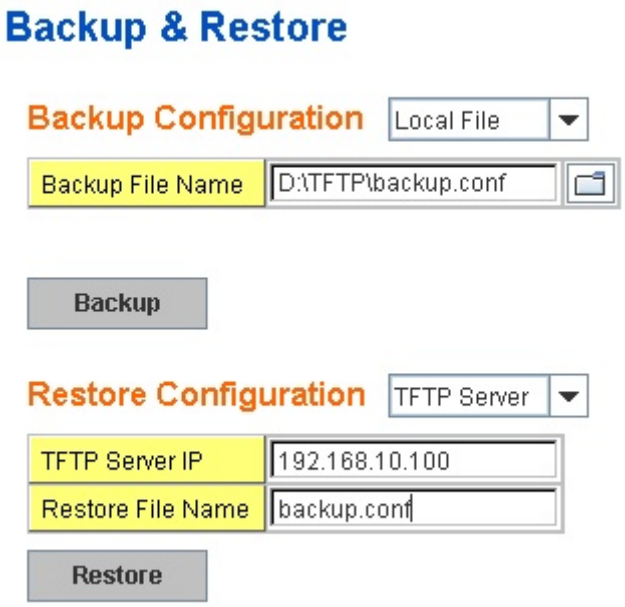
Startup Configuration File: After you have saved the running-config to flash, the new settings will be updated after a power cycle. You can use **show**

startup-config to view it in the CLI. The Backup command can only backup such configuration files to your PC or TFTP server.

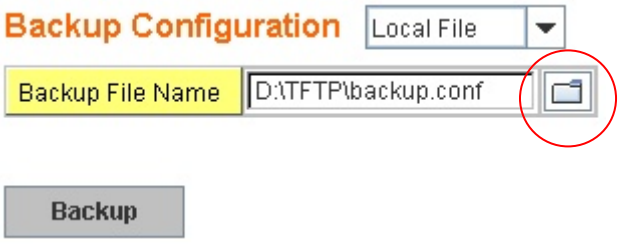
> ***Technical Tip:***
>
> ***Default Configuration File:*** *The switch provides the default configuration file in the system. You can use the Reset button, Reload command to reset the system.*
>
> ***Running Configuration File:*** *The CLI allows you to view the latest setting running on the system. The information shown here are the settings you set up but have not saved to flash. The settings not yet saved to flash will not work after a power cycle. You can* use **show running-config** to view it in the CLI.

Once you finish selecting and configuring the settings, click on **Backup** or **Restore** to run the process.

The following figure is the Main UI for Backup & Restore



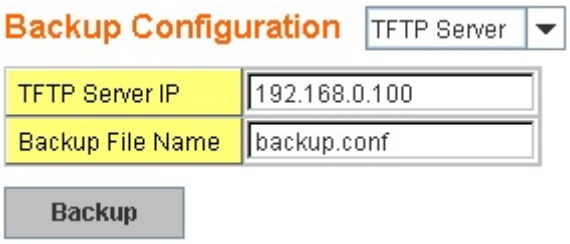
The following figure is the WEB UI for Backup/Restore Configuration - Local File mode.



Click on the Folder icon to select the target file you want to backup/restore.

Note: The folders of the path to the target file do not allow you to input space key.

The following figure is the Web UI for Backup/Restore Configuration - TFTP Server mode



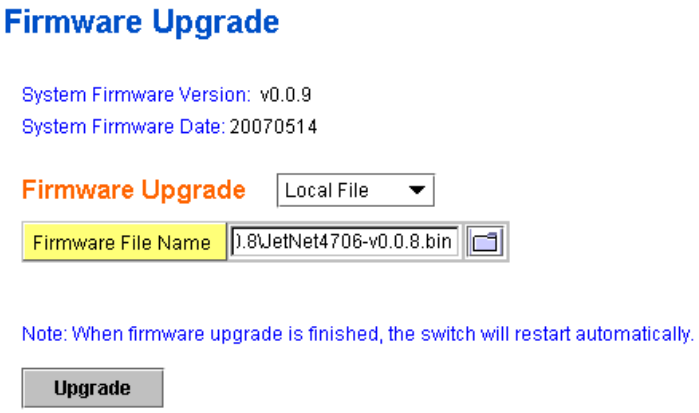
Enter the IP address of the TFTP Server. Click the Backup/Restore button.

3.2.7. Firmware Upgrade

In this section, you can update the switch with the latest firmware. *Korenix* provides the latest firmware on their Web site (www.korenix.com). New firmware may include new features, bug fixes or other software changes. The Web site also provides release notes for the update as well. We suggest you use the latest firmware *before* installing the switch.

Note: The system will automatically reboot after you finish upgrading the new firmware. Please inform all attached users before doing this.

The following figure is the Web Main UI for Firmware Upgrade.



There are 2 modes for users to backup/restore the configuration file, Local File mode and TFTP Server mode.

Local File mode — In this mode, the switch acts as the file server. Users can browse the target folder and then type in the file name to backup the configuration. Users can also browse the target folder and select the existing configuration file to restore the configuration back to the switch. This mode is only provided by Web UI; CLI is not supported.

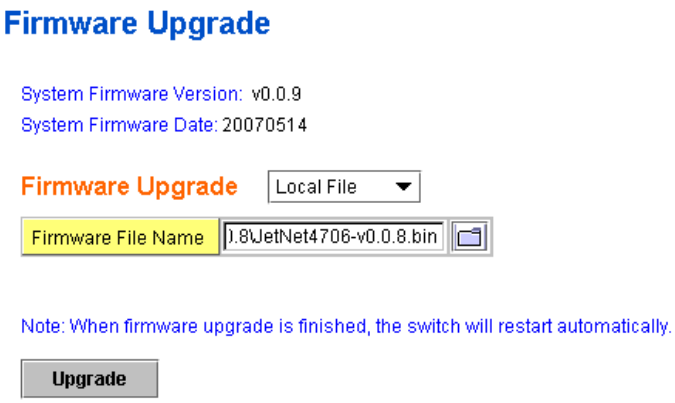
TFTP Server In this mode, the switch acts as the TFTP client. Before you do so, make sure that your TFTP server is ready. Then, type in the TFTP Server IP address. This mode can be used in both Web UI and CLI.

TFTP Server IP Address Key in the IP address of your TFTP Server here.

Firmware File Name View the file name of the new firmware.

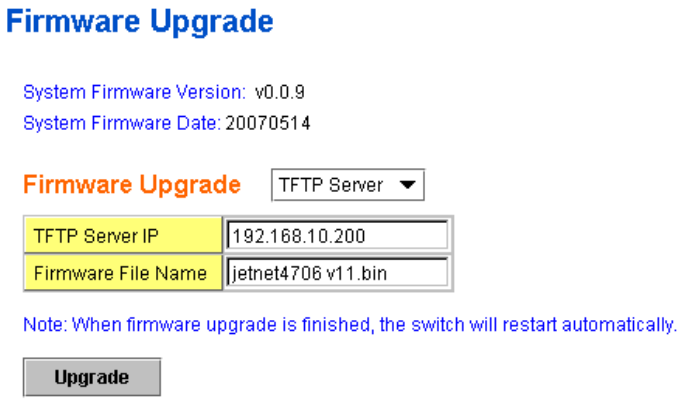
The UI also shows you the latest firmware version and build date. Please check the version number after you reboot the switch.

The following Web UI is for Firmware Upgrade - Local File mode.



Click on the Folder icon to select the correct firmware you want to upgrade

The following Web UI is for Firmware Upgrade – TFTP Server mode.



Type in the IP address of the TFTP Server and the Firmware File Name. Then click the **Upgrade** button to start the process.

After finishing the transmission of the firmware, the system will copy the firmware file and replace the firmware in the flash. The CLI will show until the process is finished.

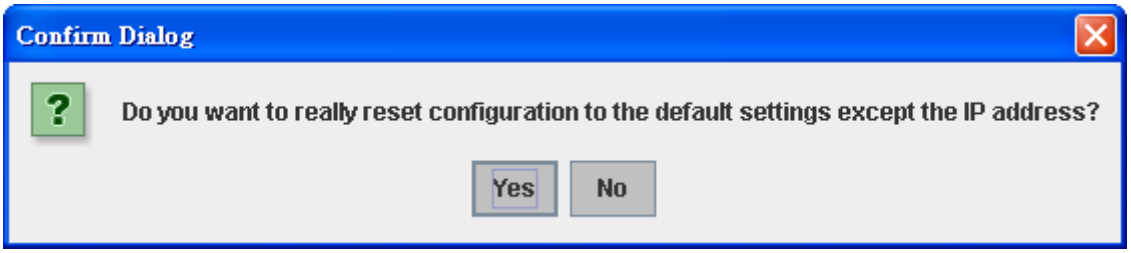
3.2.8. Factory Default

By clicking the **Reset** button, the system will reset all configurations except the IP address to its default settings. The system will show you a popup message window after running this command. Default settings will be in effect after rebooting the switch.

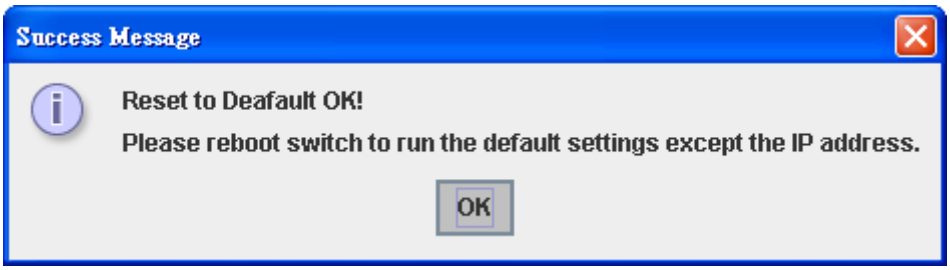
The Web UI figure for Reset to Default

Factory Default

The following figure is the popup alert screen to confirm the command. Click **Yes** to reset the system.



The following UI is a popup message screen to show you that the reset is complete. Click **OK** to close the screen. Then go to the **Reboot** page to reboot the switch.



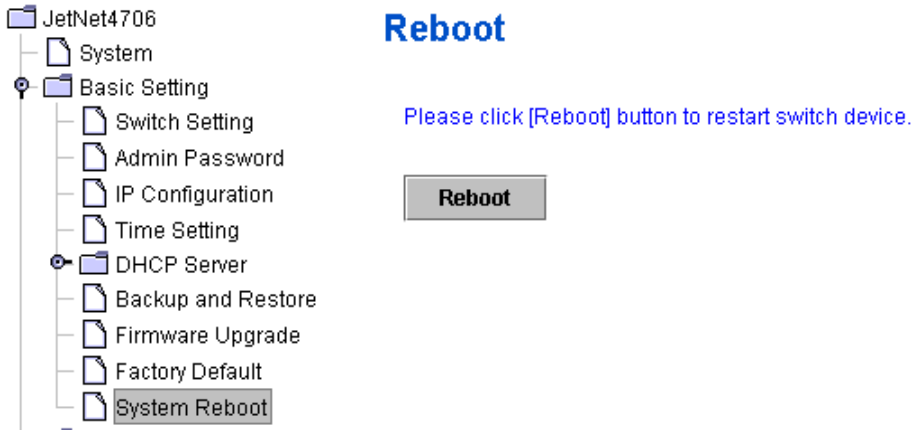
Click **OK.** The system will then automatically reboot the device.

Note: If you have already configured the IP of your device to another IP address; when you use this command through CLI and Web UI, our software will not reset

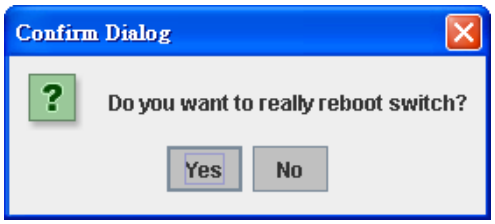
the IP address to the default IP. The system will maintain the IP address so that you can still connect to the switch via the network.

3.2.9. System Reboot

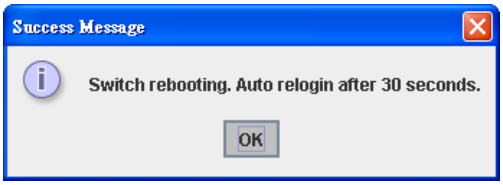
System Reboot allows you to reboot the device. Some of the feature changes require you to reboot the system. Click the **Reboot** button to reboot your device.
Note: Remember to click the **Save** button to save your settings. Otherwise, the settings you made will be gone once the switch is powered off.
Below is the Main screen for Reboot



Below is the popup alert screen to request confirmation for the Switch Reboot. Click **Yes** to reboot the switch.



The popup message screen below appears when rebooting the switch.



3.2.10. CLI Commands for Basic Settings

Feature	Command Line

Switch Setting	
System Name	Switch(config)# hostname WORD Network name of this system Switch(config)# hostname JetNet 4506-RJ Switch(config)#
System Location	Switch(config)# snmp-server location Taipei
System Contact	Switch(config)# snmp-server contact korecare@korenix.com
Display	Switch# show snmp-server name JetNet 4506-RJ Switch# show snmp-server location Taipei Switch# show snmp-server contact korecare@korenix.com Switch> show version 0.31-20061218 Switch# show hardware mac MAC Address : 00:12:77:FF:01:B0
Admin Password	
User Name and Password	Switch(config)# administrator NAME Administrator account name Switch(config)# administrator admin % Command incomplete. Switch(config)# administrator orwell PASSWORD Administrator account password Switch(config)# administrator orwell orwell Change administrator account orwell and password orwell success.
Display	Switch# show administrator Administrator account information name: orwell password: orwell
IP Configuration	
IP Address/Mask (192.168.10.8,	Switch(config)# int vlan 1 Switch(config-if)# ip address 192.168.10.8/24

255.255.255.0)	
Gateway	Switch(config)# ip route 0.0.0.0/0 192.168.10.254/24
Remove Gateway	Switch(config)# no ip route 0.0.0.0/0 192.168.10.254/24
Display	Switch# show running-config ..... ! interface vlan1 ip address 192.168.10.8/24 no shutdown ! ip route 0.0.0.0/0 192.168.10.254/24 !
Time Setting	
NTP Server	Switch(config)# ntp peer 192.168.10.100
Time Zone	Switch(config)# clock timezone 26 Sun Jan 1 04:13:24 2006 (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London Note: By typing clock timezone ?, you can see the timezone list. Then choose the number of the timezone you want to select.
Display	Switch# sh ntp associations 1 192.168.10.100 2 192.168.10.101 Switch# show clock Sun Jan 1 04:14:19 2006 (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London Switch# show clock timezone clock timezone (26) (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
DHCP Server	
DHCP server	Switch(config)# router dhcp Switch(config-dhcp)# service dhcp
Address pool	Switch(config-dhcp)# network 192.168.30.0/24 Note: the subnet ip address and mask of the address pool
Default gateway	Switch(config-dhcp)# default-router 192.168.30.1 Note: the IP address of the default gateway

Lease time (in seconds)	Switch(config-dhcp)# lease 3000
Manual binding	Switch(config-dhcp)# ip dhcp static 0012.7711.2233 192.168.30.5 Note: the client's MAC address and the IP address to be assigned
Excluded address	Switch(config-dhcp)# ip dhcp excluded-address 192.168.30.254
Display	Switch# show ip dhcp server statistics
DCHP Client	
Enable DHCP client	Switch(config)# interface vlan 1 Switch(config-if)# ip dhcp client Note: the "interface vlan" should be your management vlan.
DHCP client renew address binding	Switch(config)# interface vlan 1 Switch(config-if)# ip dhcp client renew
Display	Switch# show running-config ..... ! interface vlan1 ip dhcp client no shutdown !
DHCP Option 82 Relay Agent	
DHCP server and Relay Agent	Switch(config)# router dhcp Switch(config-dhcp)# service dhcp Switch(config-dhcp)# ip dhcp relay information option
The DHCP server the relay agent forwards to	Switch(config-dhcp)# ip dhcp helper-address 192.168.20.1
Relay policy drop	Switch(config-dhcp)# ip dhcp relay information policy
Relay policy keep	Switch(config-dhcp)# ip dhcp relay information keep
Relay policy replace	Switch(config-dhcp)# ip dhcp relay information replace
Display	Switch# show ip dhcp relay DHCP Relay Agent On ———————————— IP helper-address: 192.168.20.1 IP helper-address: 192.168.20.2 IP helper-address: 192.168.20.3 IP helper-address: 192.168.20.4 Re-forwarding policy: Replace
Backup and Restore	

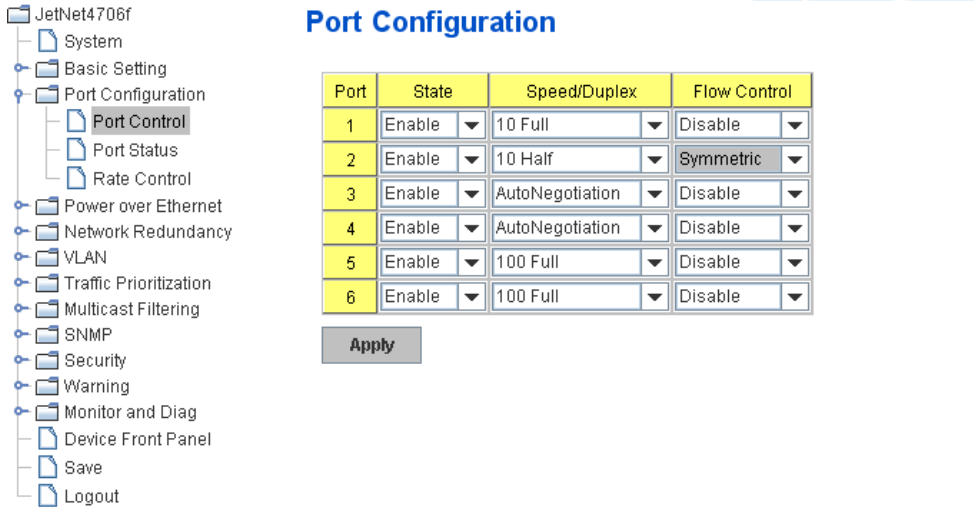
Backup Startup Configuration file	Switch# copy startup-config tftp: 192.168.10.33 Writing Configuration [OK] Note 1: To backup the latest startup configuration file, you should save current settings to flash first. You can refer to 4.12 to see how to save settings to the flash. Note 2: 192.168.10.33 is the TFTP server's IP. Your environment may use different IP addresses. Please type target TFTP server IP in this command.
Restore Configuration	Switch# copy tftp: 192.168.10.33 startup-config
Show Startup Configuration	Switch# show startup-config
Show Running Configuration	Switch# show running-config
Firmware Upgrade	
Firmware Upgrade	Switch# archive download-sw /overwrite tftp 192.168.10.33 JetNet 4506-RJ.bin Firmware upgrading, don't turn off the switch! Tftping file JetNet 4506-RJ.bin Firmware upgrading .... Firmware upgrade success!! Rebooting.....
Factory Default	
Factory Default	Switch# reload default-config file Reload OK! Switch# reboot
System Reboot	
Reboot	Switch# reboot

3.3. Port Configuration

This section shows you how to enable/disable port state, or configure port auto-negotiation, speed, duplex, flow control, rate limit control and port aggregation settings. It also allows you to view port status and aggregation information.

3.3.1. Port Control

Port Control commands allow you to enable/disable port state, or configure port auto-negotiation, speed, duplex, and flow control.



Select the port you want to configure and make changes to the port.

State Enable or disable the state of this port. Once you disable the port, it stops linking and forwarding traffic. The default setting when you receive the device is Enable, which means all the ports are working.

Speed/Duplex Configure the port speed and duplex mode of this port. Below are the selections you can choose:

Fast Ethernet Port 1~6 (fa1~fa6) : Auto Negotiation, 10M Full Duplex(10 Full), 10M Half Duplex(10 Half), 100M Full Duplex(100 Full) and 100M Half Duplex(100 Half).

The default mode is Auto Negotiation mode.

Flow Control Symmetric or disable the flow control function. “Symmetric” means that you need to activate the flow control function of the remote network device in order to let the flow control of that corresponding port on the switch work. “Disable” means that you do not need to activate the flow control function of the remote network device, as the flow control of that corresponding port on the switch will work either way.

Once you have finished configuring the settings, click the **Apply** button to save the configuration.

Note: If both ends are going at different speeds, they will not link to each other. If

both ends are in different duplex modes, they will be connected by half mode.

3.3.2. Port Status

Port Status shows you the current port status.

Port Status

Port	Type	Link	State	Speed/Duplex	Flow Control
1	100BASE	Down	Enable	--	Disable
2	100BASE	Down	Enable	--	Disable
3	100BASE	Down	Enable	--	Disable
4	100BASE	Down	Enable	--	Disable
5	100BASE-TX	Up	Enable	100 Full	Disable
6	100BASE	Down	Enable	--	Disable

A description of each column is as follows:

Port	Port interface number	
Type	100BASE for Fast Ethernet port	
Link	Link status	
	Up	Link UP
	Down	Link Down
State	Enable	State is enabled
	Disable	The port is disabled by user configured
Speed/Duplex	Current working status of the port	
Flow Control	The state of the flow control	

3.3.3. Rate Control

Rate Control

Limit Packet Type and Rate

Port	Ingress Rule		Egress Rule	
	Packet Type	Rate(Kbps)	Packet Type	Rate(Kbps)
1	Broadcast Only	8192	All	no-limit
2	Broadcast Only	8192	All	no-limit
3	Broadcast Only	8192	All	no-limit
4	Broadcast Only	8192	All	no-limit
5	Broadcast Only	8192	All	no-limit
6	Broadcast Only	8192	All	no-limit

Apply

Rate control is a form of flow control used to enforce a strict bandwidth limit of a port. You can program separate trasmitting (Egress Rule) and receiving (Ingress Rule) rate limits for each port, and even apply the limit to certain packet types as described below.

Packet Type The packet type that you want to filter. The packet types of the Ingress Rule (incoming) include Broadcast Only, Broadcast/multicast, Broadcast/Multicast/Unknown Unicast, and All. The Egress Rule (outgoing) only support All packet types.

Rate Assign the limit rate of the port. Valid values support 128Kbps, 256Kbps, 512Kbps, 1024Kbps, 2048Kbps, 4096Kbps and 8192Kbps.

To enable rate control function, please click the **Apply** button to apply the configuration.

3.3.4. Command Lines for Port Configuration

Feature	Command Line
Port Control	
Port Control – State	Switch(config-if)# shutdown -> Disable port state Port1 Link Change to DOWN interface fastethernet1 is shutdown now. Switch(config-if)# no shutdown -> Enable port state Port1 Link Change to DOWN Port1 Link Change to UP interface fastethernet1 is up now. Switch(config-if)# Port1 Link Change to UP
Port Control – Auto Negotiation	Switch(config)# interface fa1 Switch(config-if)# auto-negotiation Auto-negotiation of port 1 is enabled
Port Control – Force Speed/Duplex	Switch(config-if)# speed 100 Port1 Link Change to DOWN set the speed mode ok! Switch(config-if)# Port1 Link Change to UP Switch(config-if)# duplex full

	Port1 Link Change to DOWN set the duplex mode ok! Switch(config-if)# Port1 Link Change to UP
Port Control – Flow Control	Switch(config-if)# flowcontrol on Flowcontrol on for port 1 set ok! Switch(config-if)# flowcontrol off Flowcontrol off for port 1 set ok!
Port Status	
Port Status	Switch# show interface fa1 Interface fastethernet1 Administrative Status : Enable Operating Status : Connected Duplex : Full Speed : 100 Flow Control :off Default Port VLAN ID: 1 Ingress Filtering : Disabled Acceptable Frame Type : All Port Security : Disabled Auto Negotiation : Disable Loopback Mode : None STP Status: forwarding Default CoS Value for untagged packets is 0. Mdix mode is Disable. Medium mode is Copper. *Note: Administrative Status -> Port state of the port.* *Operating status -> Current status of the port. Duplex ->* *Duplex mode of the port. Speed -> Speed mode of the port.* *Flow control -> Flow Control status of the port.*
Rate Control	
Rate Control – Ingress or Egress	Switch(config-if)# rate-limit egress Outgoing packets ingress Incoming packets *Note: To enable rate control, you should select the Ingress or Egress rule first; then assign the packet type and bandwidth.*

Rate Control – Filter Packet Type	Switch(config-if)# rate-limit ingress mode all Limit all frames broadcast Limit Broadcast frames flooded-unicast Limit Broadcast, Multicast and flooded unicast frames multicast Limit Broadcast and Multicast frames Switch(config-if)# rate-limit ingress mode broadcast Set the ingress limit mode broadcast ok.
Rate Control - Bandwidth	Switch(config-if)# rate-limit ingress bandwidth 0 0 is no limit 1024 1024 is 1024Kbps 128 128 is 128Kbps 2048 2048 is 2048Kbps 256 256 is 256Kbps 4096 4096 is 4096Kbps 512 512 is 512Kbps 8192 8192 is 8192Kbps Switch(config-if)# rate-limit ingress bandwidth 8192 Set the ingress rate limit to 8192k for Port 1.

3.4. Network Redundancy

It is critical for industrial applications for networks to continue working non-stop. This switch supports standard RSTP, Multiple Super Ring, Rapid Dual Homing and Legacy Super Ring Client modes.

Multiple Super Ring (MSR) technology is Korenix's 3rd generation Ring redundancy technology. This is patented and protected by Korenix and is used all over the world. MSR ranks the fastest restore and failover time, 0 ms for restore and less than 5 milliseconds for failover.

Advanced Rapid Dual Homing technology also facilitates this switch to connect with a core managed switch via standard Rapid Spanning Tree Protocol. With RDH technology, you can also run RSTP to couple several Rapid Super Rings, which is also known as Auto Ring Coupling.

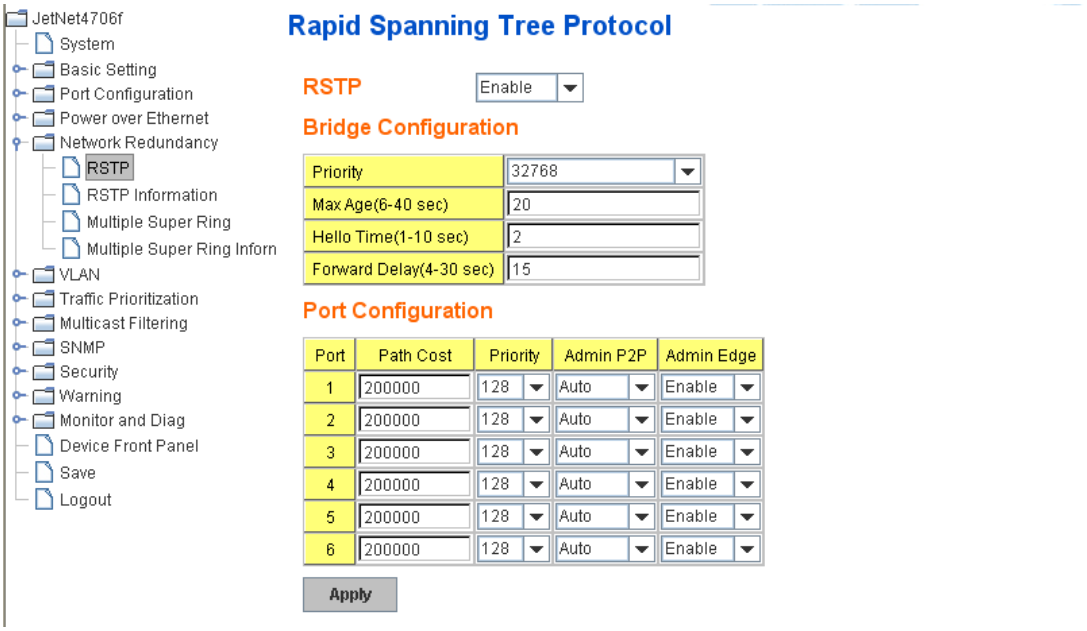
To become backwards compatible with the Legacy Super Ring technology implemented in JetNet 4000/4500 switches, this switch also supports Super Ring Client mode. The Super Ring ports can pass through Super Ring control packets extremely well and works with Super Ring.

Besides Korenix ring technology, this switch also supports 802.1D-2004 version Rapid Spanning Tree Protocol (RSTP). The new version of RSTP standard includes 802.1D-1998 STP, 802.1w RSTP.

3.4.1. RSTP

RSTP stands for Rapid Spanning Tree Protocol. If a switch has more than one path to a destination, it will lead to message loops that can generate broadcast storms and quickly bog down a network. The spanning tree was created to combat the negative effects of message loops in switched networks. A spanning tree uses a spanning tree algorithm (STA) to automatically sense whether a switch has more than one way to communicate with a node. It will then select the best path (primary), and block the other path(s). It will also keep track of the blocked path(s) in case the primary path fails. Spanning Tree Protocol (STP) introduced a standard method to accomplish this. It is specified in IEEE 802.1D-1998. Later, Rapid Spanning Tree Protocol (RSTP) was adopted and represents the evolution of STP, providing for a much faster spanning tree convergence after a topology change. This is specified in IEEE 802.1w. In 2004, 802.1w was included into the 802.1D-2004 version. This switch supports both RSTP and STP (all switches that supports RSTP are also backwards compatible with switches that support only STP).

This page allows you to enable/disable RSTP, and configure the global setting and port settings.



RSTP Mode You must first enable STP/RSTP mode before configuring any related parameters. Parameter settings required for both STP

and RSTP are the same. Note that 802.1d refers to STP mode, while 802.1w refers to faster RSTP mode.

Bridge Configuration

Priority (0-61440) RSTP uses bridge ID to determine the root bridge, the bridge with the highest bridge ID becomes the root bridge. The bridge ID is composed of bridge priority and bridge MAC address. So that the bridge with the highest priority becomes the highest bridge ID. If all of the bridge IDs have the same priority, the bridge with the lowest MAC address will then become the root bridge.

Note: The bridge priority value must be in multiples of 4096. A device with a lower number has a higher bridge priority. Ex: 4096 is higher than 32768.

Max Age (6-40) Enter a value from 6 to 40 seconds here. This value represents the time that a bridge will wait without receiving Spanning Tree Protocol configuration messages before attempting to reconfigure. If this switch is not the root bridge, and if it has not received a hello message from the root bridge in the amount of time equal to the Max Age, then this switch will reconfigure itself as a root bridge. Once two or more devices on the network are recognized as a root bridge, the devices will renegotiate to set up a new spanning tree topology.

Hello Time (1-10) Enter a value from 1 to 10 seconds here. This is a periodic timer that drives the switch to send out a BPDU (Bridge Protocol Data Unit) packet to check current STP status. The root bridge of the spanning tree topology periodically sends out a "hello" message to other devices on the network to check if the topology is "healthy." The "hello time" is the amount of time the root has waited in between sending hello messages.

Forward Delay Time (4-30) Enter a value between 4 and 30 seconds. This

value is the time that a port waits before changing from Spanning Tree Protocol learning and listening states to forwarding state. This is the amount of time this switch will wait before checking to see if it should be changed to a different state.

Once you have completed your configuration, click the Apply button to apply your settings.

Note: You must observe the following rules to configure Hello Time, Forwarding Delay, and Max Age parameters.

2 × (Forward Delay Time – 1 sec) >= Max Age Time >= 2 × (Hello Time value + 1 sec)

Port Configuration

Select the port you want to configure; you will be able to view the current settings and status of the port.

Path Cost Enter a number between 1 and 200,000,000. This value represents the "cost" of the path to the other bridge from the transmitting bridge at the specified port.

Priority Enter a value between 0 and 240 using multiples of 16. This is the value that decides which port should be blocked by priority in a LAN.

Admin P2P Some of the rapid state transitions that are possible within RSTP depend upon whether the port of concern can only be connected to another bridge (i.e. it is served by a point-to-point LAN segment), or if it can be connected to two or more bridges (i.e. it is served by a shared-medium LAN segment). This function allows P2P status of the link to be manipulated administratively. Auto means to auto select P2P or Share mode. P2P means P2P is enabled, while Share means P2P is disabled.

Admin Edge A port directly connected to the end stations cannot create a bridging loop in the network. To configure this port as an edge port, set the port to the Enable state. When the non-bridge device connects an admin edge port, this port will be in blocking state and turn to forwarding state in 4 seconds.

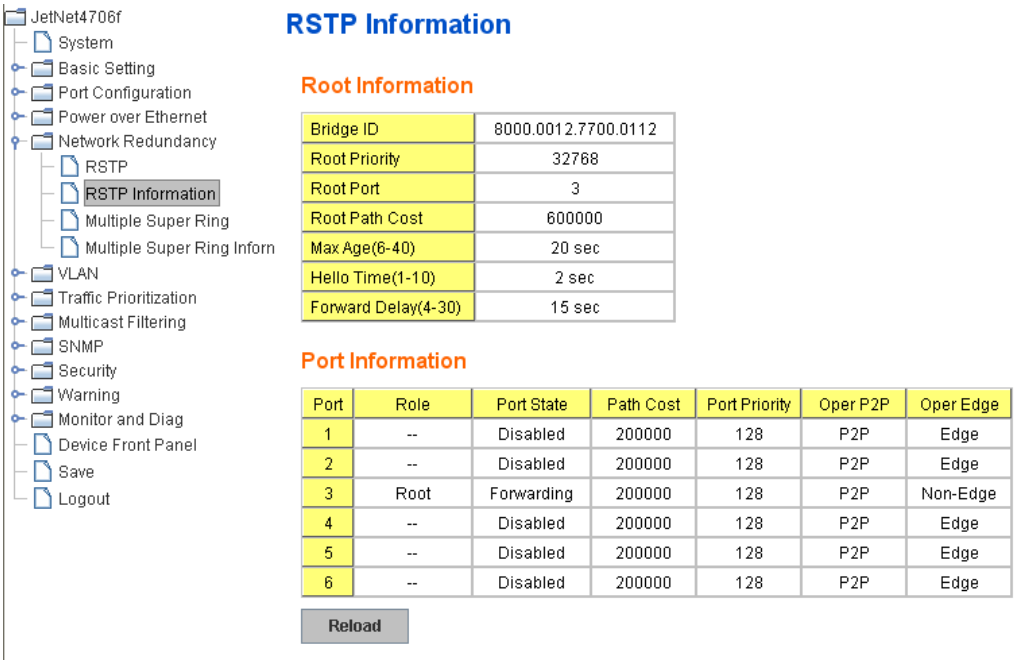
Once you have finished your configuration, click the Apply button to save your settings.

3.4.2. RSTP Information

This page allows you to see the information of the root switch and port status.

Root Information You can see Root Bridge ID, Root Priority, Root Port, Root Path Cost and the Max Age, Hello Time and Forward Delay of BPDU sent from the root switch.

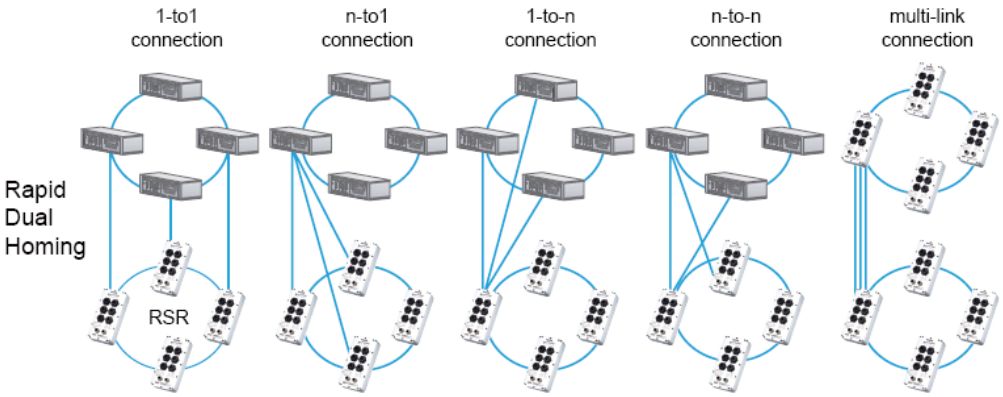
Port Information You can see port Role, Port State, Path Cost, Port Priority, Oper P2P mode, Oper edge port mode.



3.4.3. Multiple Super Ring (MSR)

The most common industrial network redundancy is to form a ring or loop. Typically, the managed switches are connected in a series and the last switch is connected back to the first one. In such a connection, you can use Korenix Super Ring and Rapid Super Ring technology.

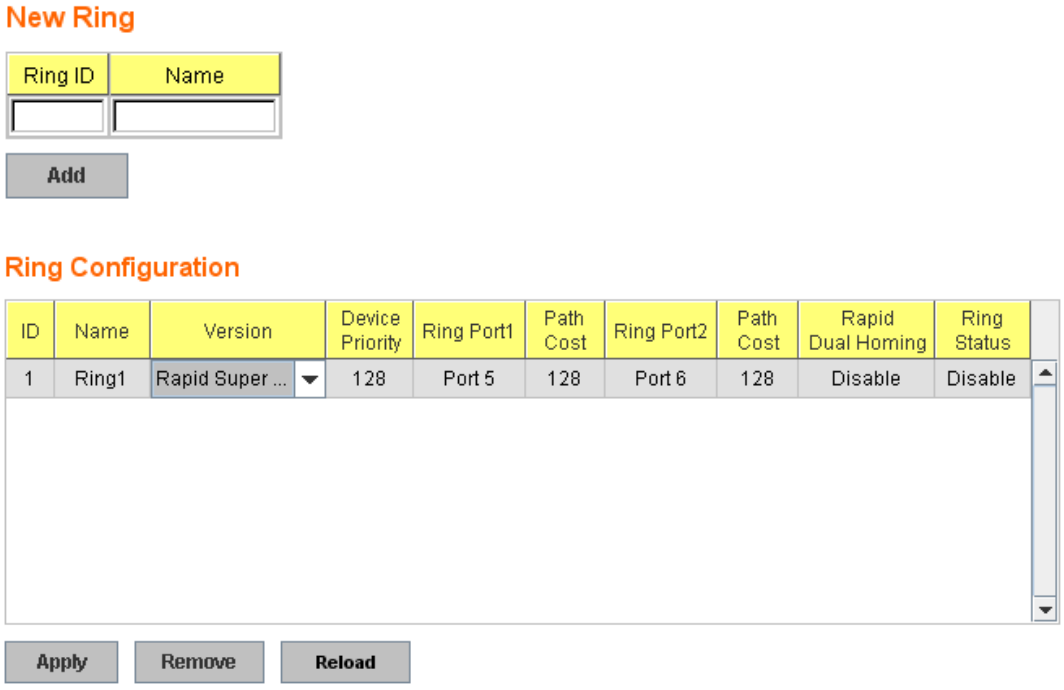
Super Ring is Korenix's 1st generation ring redundancy technology released with JetNet 4000/4500. Rapid Super Ring (RSR) is Korenix's 2nd generation Ring redundancy technology. The Rapid Super Ring has an enhanced Ring Master selection and shorter recovery time. Mutilple Super Ring is the 3rd Korenix Ring technology. It is designed for more complex ring application and even faster recovery time. These are patented and protected by Korenix and is used in countries all over the world.



This page allows you to enable the settings for Multiple Super Ring and Rapid Dual Homing.

New Ring To create a Rapid Super Ring. Just fill in the Ring ID which has a range from 0 to 31. If the name field is left blank, the name of this ring will automatically name with RingID.

Note: Only JetNet 5000 series and upper can create more than one ring.



This page allows you to enable the settings for Rapid Super Ring.

Ring Configuration

ID Once a Ring is created, This appears and can not be changed.

Name This field will show the name of the Ring. If it is not filled in when creating, it will be automatically named by the rule “RingID”.

Version	The version of Ring can be changed here. There are two modes to choose: Rapid Super Ring as default and Super ring for compatible with Korenix 1st general ring.
Device Priority	The switch with highest priority (highest value) will be automatically selected as Ring Master. Then one of the ring ports in this switch will become forwarding port and the other one will become blocking port. If all of the switches have the same priority, the switch with the biggest MAC address will be selected as Ring Master.
Ring Port1	In Rapid Super Ring environment, you should have 2 Ring Ports. No matter this switch is Ring Master or not, when configuring RSR, 2 ports should be selected to be Ring Ports. For Ring Master, one of the ring ports will become the forwarding port and the other one will become the blocking port.
Path Cost	Change the Path Cost of Ring Port1. If this switch is the Ring Master of a Ring, then it determines the blocking port. The Port with higher Path Cost in the two ring Ports will become the blocking port, if the Path Cost is the same, the port with larger port number will become the blocking port.
Ring Port2	Assign another port for ring connection
Path Cost	Change the Path Cost of Ring Port2
Rapid Dual Homing	Rapid Dual Homing is an important feature of Korenix 3rd generation Ring redundancy technology. When you want to connect multiple RSR or form redundant topologies with other vendors, Rapid Dual Homing could allow you to have multiple links for redundancy without any problem. The maximum uplink is 7 per group. In Dual Homing I released with JetNet 4000/4500 series, you have to configure additional port as Dual Homing port to two uplink switches. In Rapid Dual Homing, you don't need to configure specific port to connect to other protocol. The Rapid Dual Homing will smartly choose the fastest link for primary link and block all the other links to avoid loop. If the primary link failed, Rapid Dual Homing will automatically forward the secondary link for network redundant. Of course, if there are more

connections, they will be standby links and recover one of then if both primary and secondary links are broken.

Ring status To enable/disable the Ring. Please remember to enable the ring after you add it.

3.4.4. Ring Information

This page shows MSR information.

ID Ring ID.

Version The version of the ring, either Rapid Super Ring or Super Ring

Role This Switch is RM or nonRM

Status If this field is Normal which means the redundancy is approved. If any one of the link in this Ring is broken, then the status will be Abnormal.

RM MAC The MAC address of Ring Master of this Ring. It helps to find the redundant path.

Blocking Port This field shows which port of RM.is blocked.

Role Transition Count This means how many times this switch has changed its Role from nonRM to RM or from RM to nonRM.

Role state Transition Count This number means how many times the Ring status has been transformed between Normal and Abnormal state.

3.4.5. Command Lines for Network Redundancy

Feature	Command Line
RSTP	
Enable	Switch(config)# spanning-tree enable
Disable	Switchconfig)# spanning-tree disable
RSTP mode	Switch(config)# spanning-tree mode rapid-stp Spanning Tree Mode change to be RSTP (802.1w).
STP mode	Switch(config)# spanning-tree mode stp Spanning Tree Mode change to be STP (802.1d).
Priority	Switch(config)# spanning-tree priority <0-61440> valid range is 0 to 61440 in multiple of 4096 Switch(config)# spanning-tree priority 4096
Max Age	Switch(config)# spanning-tree max-age <6-40> Valid range is 6~40 seconds Switch(config)# spanning-tree max-age 10
Hello Time	Switch(config)# spanning-tree hello-time <1-10> Valid range is 1~10 seconds Switch(config)# spanning-tree hello-time 2
Forward Delay	Switch(config)# spanning-tree forward-time <4-30> Valid range is 4~30 seconds Switch(config)# spanning-tree forward-time 15
algorithm-timer	Switch(config)# spanning-tree algorithm-timer *forward delay, max-age, hello time.* Switch(config)# spanning-tree algorithm-timer 15 20 2
Path Cost Method	Switch(config-if)# spanning-tree cost method long ->specifies 32-bit based values that range from 1-200,000,000 short ->specifies 16-bit based values that range from 1-65535 Switch(config-if)# spanning-tree cost method long
Port Priority	Switch(config-if)# spanning-tree port-priority <0-240> Number from 0 to 240, in multiple of 16 Switch(config-if)# spanning-tree port-priority 128
bpdufilter	Switch(config-if)# spanning-tree bpdufilter enable
bpduguard	Switch(config-if)# spanning-tree bpduguard enable
Link Type - Auto	Switch(config-if)# spanning-tree link-type auto
Link Type - P2P	Switch(config-if)# spanning-tree link-type point-to-point

Link Type – Share	Switch(config-if)# spanning-tree link-type shared
Edge Port	Switch(config-if)# spanning-tree edge-port enable Switch(config-if)# spanning-tree edge-port disable
RSTP Info	
Active status	Switch# show spanning-tree active Rapid Spanning-Tree feature Enabled Spanning-Tree BPDU transmission-limit 3 Root Address 0012.7701.0386 Priority 4096 Root Path Cost : 200000 Root Port : 7 Root Times : max-age 20 sec, hello-time 2 sec, forward-delay 15 sec Bridge Address 0012.77ff.0102 Priority 4096 Bridge Times : max-age 10 sec, hello-time 2 sec, forward-delay 15 sec Aging time : 300 Port Role Port-State Cost Prio.Nbr Type ---- ---- ---- ---- ---- ---- fa6 Designated Forwarding 200000 128.6 Auto(RST) fa7 Root Forwarding 200000 128.7 Shared(STP)
RSTP Summary	Switch# show spanning-tree summary Switch is in rapid-stp mode. BPDU skewing detection disabled for the bridge. Backbonefast disabled for bridge. Summary of connected spanning tree ports : #Port-State Summary Blocking Listening Learning Forwarding Disabled ---- ---- ---- ---- ---- 0 0 0 2 8 #Port Link-Type Summary AutoDetected PointToPoint SharedLink EdgePort ---- ---- ---- ---- 9 0 1 9
Port Info	Switch# show spanning-tree port detail fa7 (Interface_ID) Rapid Spanning-Tree feature Enabled IEEE compatible Spanning-Tree Protocol Enabled

	Spanning-Tree BPDU transmission-limit 3 Bridge identifier has priority 4096, address 0012.77ff.0102 Configured hello time 2, max age 10, forward delay 15 Current root has priority 4096, address 0012.7701.0386 Root port is 7 , cost of root path is 200000 Topology change flag not set, detected flag not set Number of topology changes 0, last change occurred from 0000.0000.0000 Times: hello 2 , max age 20 , forward delay 15 Timers: hello 0 , topology change 0 Rapid Spanning-Tree link-type : Shared Rapid Spanning-Tree edge-port : Disabled Port 128.7 as Root Role is in Forwarding State Port Path Cost 200000, Port Identifier 128.7 Designated root has priority 4096, address 0012.7701.0386 Designated bridge has priority 4096, address 0012.7701.0386 Designated Port ID is 128.1, Root Path Cost is 0 Timers : message-age 4 sec, forward-delay 0 sec Forwarding-State Transmit count 2 BPDU: sent 624 , received 3600 TCN : sent 0 , received 0
Rapid Super Ring	
Create or configure a Ring	Switch(config)# multiple-super-ring 1 Ring 1 created Switch(config-super-ring-plus)# *Note: 1 is the target Ring ID which is going to be created or configured.*
Super Ring Version	Switch(config-super-ring-plus)# version default set default to rapid super ring rapid-super-ring rapid super ring super-ring super ring Switch(config-super-ring-plus)# version rapid-super-ring
Priority	Switch(config-super-ring-plus)# priority <0-255> valid range is 0 to 255 default set default Switch(config-super-ring-plus)# priority 100
Ring Port	Switch(config-super-ring-plus)# port IFLIST Interface list, ex: fa1,fa3-5,fa8-10

	cost path cost Switch(config)# super-ring port fa1,fa2
Ring Port Cost	Switch(config-super-ring-plus)# port cost <0-255> valid range is 0 or 255 default set default (128)valid range is 0 or 255 Switch(config-super-ring-plus)# port cost 100 <0-255> valid range is 0 or 255 default set default (128)valid range is 0 or 255 Switch(config-super-ring-plus)# port cost 100 200 Set path cost success.
Rapid Dual Homing	Switch(config-super-ring-plus)# rapid dual-homing enable Switch(config-super-ring-plus)# rapid dual-homing disable Switch(config-super-ring-plus)# rapid dual-homing port IFLIST Interface name, ex: fastethernet1 or fa8 auto-detect up link auto detection IFNAME Interface name, ex: fastethernet1 or fa4 Switch(config-super-ring-plus)# rapid dual-homing port fa3,fa5-6 set Dual Homing port success. Switch(config-multiple-super-ring)# rapid-dual-homing port fa1 priority default Set Rapid Dual Homing port priority success. *Note: auto-detect is recommended for Rapid Ddual Homing.* *Note: When configure Rapid Dual Homing port, IFNAME is used for port priority.*
Ring Info	
Ring Info	Switch# show multiple-super-ring [Ring ID] [Ring1] Ring1 Current Status : Disabled Role : Disabled Ring Status : Abnormal Ring Manager : 0000.0000.0000 Blocking Port : N/A Giga Copper : N/A Configuration :

	Version : Rapid Super Ring Priority : 128 Ring Port : fa1, fa2 Path Cost : 100, 200 Rapid Dual Homing: Disabled Statistics : Watchdog sent 0, received 0, missed 0 Link Up sent 0, received 0 Link Down sent 0, received 0 Role Transition count 0 Ring State Transition count 1 Ring ID is optional. If the ring ID is typed, this command will only display the information of the target Ring.

3.5. VLAN

This switch supports Port-Based VLAN functionality for the purpose of limiting a broadcast domain to specific members of a group by physically grouping the members together.

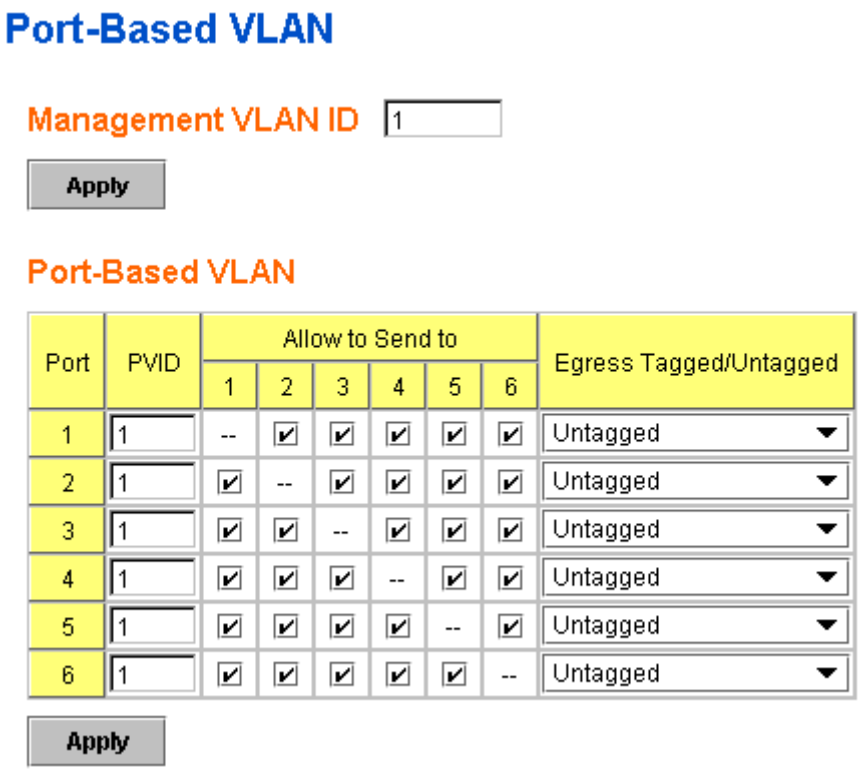
The device determines the membership of a frame by examining the configuration of the port that receives the frame, or by reading the frame's VLAN tag. A four-byte field in the header is used to identify the VLAN. This VLAN identification indicates which VLAN the frame belongs to. If the frame has no tag header, the switch checks the VLAN setting of the port that received the frame. If the switch has been configured for port based VLAN support, it assigns the port's VLAN identification to the new frame.

3.5.1. Management VLAN

The Management VLAN ID configuration is for the switch management interface security. Only the management packet with the same VLAN ID will forward to a CPU interface. You can assign an ID number from 1 to 4094, and then click the Apply button to assign Management VLAN ID. The following is the UI interface.

3.5.2. Port-Based VLAN Configuration

The following figure is the Web user interface for a Port-Based VLAN.



PVID

The abbreviation of Port VLAN ID. Enter the port VLAN ID here. PVID allows the switches to identify which port belongs to which VLAN. To keep things simple, it is recommended that PVID is equivalent to VLAN IDs. The values of PVIDs are from 1 to 4094. But, 0 and 4095 are reserved. You can not input these 2 PVIDs. 1 is the default value. 2 to 4094 are valid and available in this column. Type the PVID you'd like to configure here.

Allow Send To

This column defines the port that traffic could be forwarded to. You can click the icon to join the port as a Port Based VLAN group. The following figure is the Web user interface for Port-Based VLAN configuration.

Egress Tagged/ Untagged

Each port supports Tag modify function. It includes Untagged, Tagged or Un-modify modes. The packets egress from this port is modified according to the

selected rule.

3.5.3. CLI Commands of the VLAN

Command Lines of the VLAN port configuration, VLAN configuration and VLAN table display

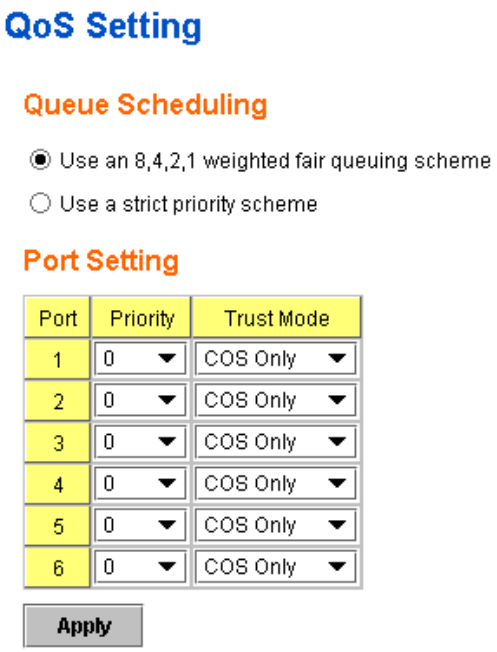
Description	CLI Command
Displays the current port based vlan configuration for each port, which include the default PVID, the ports for forwarding, and the egress mode of the port.	show vlan ex: Switch# sh vlan Port-based vlan mode: Port PVID EgressMode Egress Ports — — ——— —————— fa1 1 Tagged fa2-3 fa2 1 Untagged fa3-4 fa3 1 Untagged fa1-2,fa4-6 fa4 1 Untagged fa1-3,fa5-6 fa5 3 Untagged fa1-4,fa6 fa6 1 Untagged fa1-5 Switch#
The ports where the frame comes in to this port are allowed to forward to.	switchport port-based-vlan egress-ports [IFLIST] ex: port 1 can forward packet to port 2,3 Switch(config-if)# switchport port-based-vlan egress-ports fa2,fa3 Set port-based vlan success
Assign default PVID for this port	switchport trunk native vlan VID ex: assign VID 1 to port 1 Switch# configure terminal Switch(config)# interface fa1 Switch(config-if)# switchport trunk native vlan 1 Set port default vlan id to 1 success Switch(config-if)#
Specify when a frame that is egressing from this port should be tagged, untagged or unmodified	switchport port-based-vlan mode (untagged|tagged|unmodified) ex: Egress packet of port 1 with tagged. Switch(config-if)# switchport port-based-vlan mode tagged Set port-based vlan mode success

3.6. Traffic Prioritization

Quality of Service (QoS) provides a traffic prioritization mechanism that allows users to deliver better service to certain flows. QoS can also help to alleviate congestion problems and ensure that high priority traffic is delivered first. This section allows you to configure Traffic Prioritization settings for each port in regards to setting priorities.

This switch supports 4 physical queues, weighted fair queuing (WRR) and Strict Priority scheme, which follows 802.1p COS tag and IPv4 TOS/DiffServ information to prioritize the traffic of your industrial network.

3.6.1. QoS Setting



Queue Scheduling

Use an 8,4,2,1 weighted fair queuing scheme. This is also known as WRR (Weight Round Robin). JetNet will follow the 8:4:2:1 rate to process the packets in a queue from the highest priority to the lowest. For example, the system will simultaneously process 8 packets with the highest priority in the queue, 4 packets with middle priority, 2 packets with low priority, and 1 packet with the lowest priority.

Use a strict priority scheme. Packets with the highest priority in the queue will always be processed first.

Port Setting

Priority Indicate the default port priority value for untagged or priority-tagged frames. When the switch receives the frames, it will assign the priority to the frames. You can enable 0, 1, 2 or 3 to the port. The priority is directly mapping to queue id, queue 3 is the highest priority queue.

Trust Mode This indicates Queue Mapping types for you to select.

- **CoS Only** Port priority will only follow CoS-Queue Mapping that you have assigned.
- **DSCP Only** Port priority will only follow DSCP-Queue Mapping that you have assigned.
- **CoS first** Port priority will follow CoS-Queue Mapping first, and then DSCP-Queue Mapping rule.
- **DSCP first** Port priority will follow DSCP-Queue Mapping first, and then CoS-Queue Mapping rule.
- **Port Based** The port priority will follow the queue priority that you have assigned.

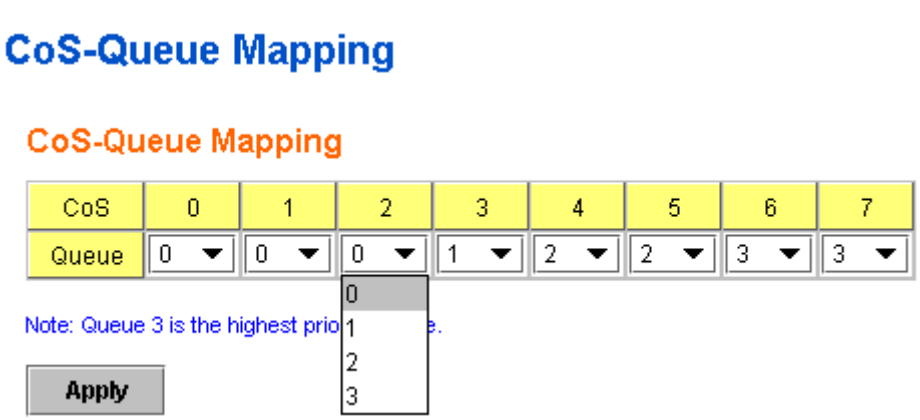
The default priority type is CoS Only. The system will provide a default CoS-Queue table that you can refer to for the next command.

After configuring, click the Apply button to enable the settings.

3.6.2. CoS-Queue Mapping

This area is where you can set CoS values to the Physical Queue mapping table. Since the switch supports 4 physical queues (Lowest, Low, Middle and High), each CoS value should be assigned to a level of the physical queue.

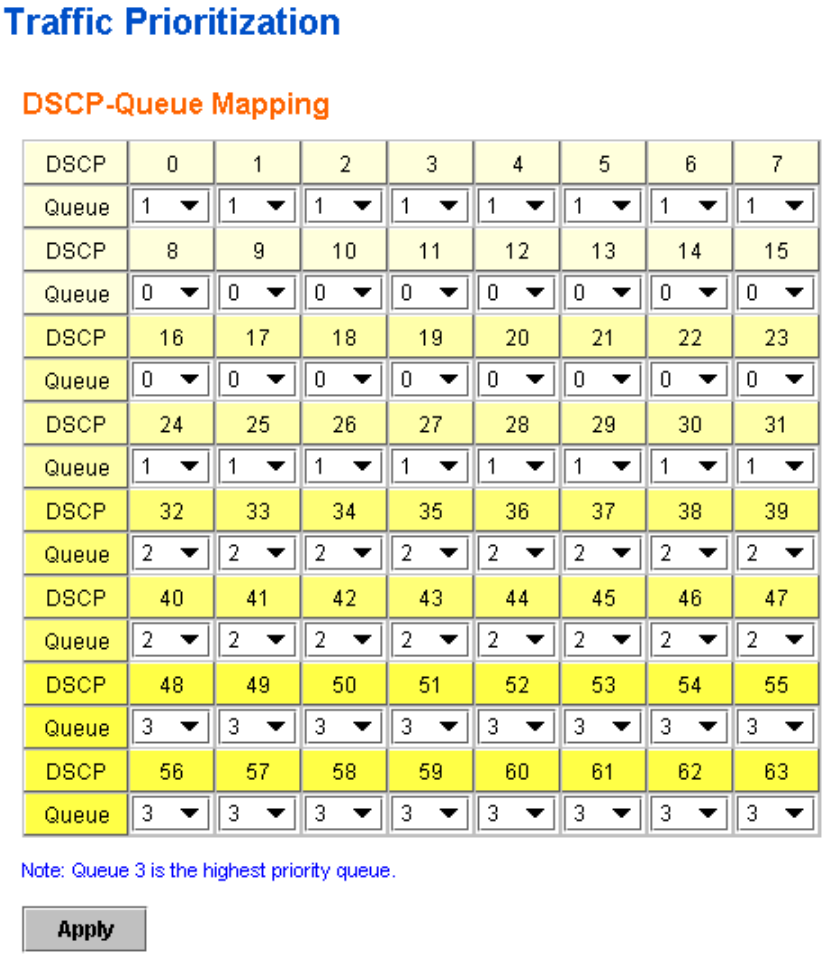
You can easily assign the mapping table or follow suggestions from the 802.1p standard. *Korenix* uses 802.p standards by default. You will find that the CoS values 1 and 2 are mapped to physical Queue 0 (lowest queue). CoS values 0 and 3 are mapped to physical Queue 1, (low/normal physical queue), CoS values 4 and 5 are mapped to physical Queue 2 (middle physical queue), and CoS values 6 and 7 are mapped to physical Queue 3 (highest physical queue).



After configuring, click the Apply button to enable the settings.

3.6.3. DSCP-Queue Mapping

DSCP-Queue mapping is a table which maps the DSCP values to the physical queues. There are 4 physical queues treating outgoing frame in 4 priorities: lowest, low, middle and high. Changing the mapping between the DSCP value and the priority queue for the quality of service you need.



After configuring, click the **Apply** button to enable the settings.

3.6.4. CLI Commands for Traffic Prioritization

Feature	Command Line
QoS Setting	
Queue Scheduling – Strict Priority	Switch(config)# qos queue-sched sp Strict Priority wrr Weighted Round Robin (Use an 8,4,2,1 weight) Switch(config)# qos queue-sched sp <cr>
Queue Scheduling - WRR	Switch (config)# qos queue-sched wrr
Port Setting – priority (Default Port Priority)	Switch(config)# interface fa1 Switch(config-if)# qos priority DEFAULT-PRIORITY Assign an priority (3 highest) Switch(config-if)# qos cos 3 The default port priority value is set 3 ok. *Note: When change the port setting, you should Select the specific port first. Ex: fa1 means fast Ethernet port 1.*
Port Setting – Trust Mode- CoS Only	Switch(config)# interface fa1 Switch(config-if)# qos trust cos The port trust is set CoS only ok.
Port Setting – Trust Mode- CoS Frist	Switch(config)# interface fa1 Switch(config-if)# qos trust cos-first The port trust is set CoS first ok.
Port Setting – Trust Mode- DSCP Only	Switch(config)# interface fa1 Switch(config-if)# qos trust dscp The port trust is set DSCP only ok.
Port Setting – Trust Mode- DSCP First	Switch(config)# interface fa1 Switch(config-if)# qos trust dscp-first The port trust is set DSCP first ok.
Port Setting – Trust Mode- Port Based	Switch(config)# interface fa1 Switch(config-if)# qos trust port-based The port trust is set port based ok.
Display – Queue Scheduling	Switch# show qos queue-sched QoS queue scheduling scheme : Weighted Round Robin (Use an 8,4,2,1 weight)
Display – Port Setting - Trust	Switch# show qos trust

Mode	QoS Port Trust Mode : Port Trust Mode —+——— 1 DSCP first 2 COS only 3 COS only 4 COS only 5 COS only 6 COS only 7 COS only 8 COS only 9 COS only 10 COS only
Display – Port Setting – CoS (Port Default Priority)	Switch# show qos port-cos Port Default Cos : Port CoS —+— 1 0 2 0 3 0 4 0 5 0 6 0
CoS-Queue Mapping	
Format	Switch(config)# qos cos-map PRIORITY Assign an priority (7 highest) Switch(config)# qos cos-map 1 QUEUE Assign an queue (0-3) *Note: qos cos-map priority_value queue_value*
Map CoS 0 to Queue 1	Switch(config)# qos cos-map 0 1 The CoS to queue mapping is set ok.
Map CoS 1 to Queue 0	Switch(config)# qos cos-map 1 0 The CoS to queue mapping is set ok.
Map CoS 2 to Queue 0	Switch(config)# qos cos-map 2 0 The CoS to queue mapping is set ok.
Map CoS 3 to Queue 1	Switch(config)# qos cos-map 3 1

	The CoS to queue mapping is set ok.
Map CoS 4 to Queue 2	Switch(config)# qos cos-map 4 2 The CoS to queue mapping is set ok.
Map CoS 5 to Queue 2	Switch(config)# qos cos-map 5 2 The CoS to queue mapping is set ok.
Map CoS 6 to Queue 3	Switch(config)# qos cos-map 6 3 The CoS to queue mapping is set ok.
Map CoS 7 to Queue 3	Switch(config)# qos cos-map 7 3 The CoS to queue mapping is set ok.
Display – CoS-Queue mapping	Switch# sh qos cos-map CoS to Queue Mapping : CoS Queue —— + —— 0 1 1 0 2 0 3 1 4 2 5 2 6 3 7 3
DSCP-Queue Mapping	
Format	Switch(config)# qos dscp-map PRIORITY Assign an priority (63 highest) Switch(config)# qos dscp-map 0 QUEUE Assign an queue (0-3) *Note: qos dscp-map priority_value queue_value*
Map DSCP 0 to Queue 1	Switch (config)# qos dscp-map 0 1 The TOS/DSCP to queue mapping is set ok.
Display – DSCO-Queue mapping	Switch# show qos dscp-map DSCP to Queue Mapping : (dscp = d1 d2) d2| 0 1 2 3 4 5 6 7 8 9 d1 | ——+—————— 0 | 1 1 1 1 1 1 1 1 0 0 1 | 0 0 0 0 0 0 0 0 0 0

	2 | 0 0 0 0 1 1 1 1 1 1 3 | 1 1 2 2 2 2 2 2 2 2 4 | 2 2 2 2 2 2 2 2 3 3 5 | 3 3 3 3 3 3 3 3 3 3 6 | 3 3 3 3

3.7. Multicast Filtering

For multicast filtering, the device uses IGMP Snooping technology. The IGMP (Internet Group Management Protocol) is an Internet Protocol that provides a way for an internet device to report its multicast group membership to adjacent routers. Multicasting allows one computer on the internet to send data to a multitude of other computers that have identified themselves as being interested in receiving the originating computers data.

Multicasting is useful for such applications as updating the address books of mobile computer users in the field, sending out newsletters to a distribution list, and broadcasting streaming media to an audience that has tuned into the event by setting up multicast group membership.

In effect, IGMP Snooping manages multicast traffic by making use of switches, routers, and hosts that support IGMP. Enabling IGMP Snooping allows the ports to detect IGMP queries, report packets, and manage multicast traffic through the switch. IGMP has three fundamental types of messages, as shown below:

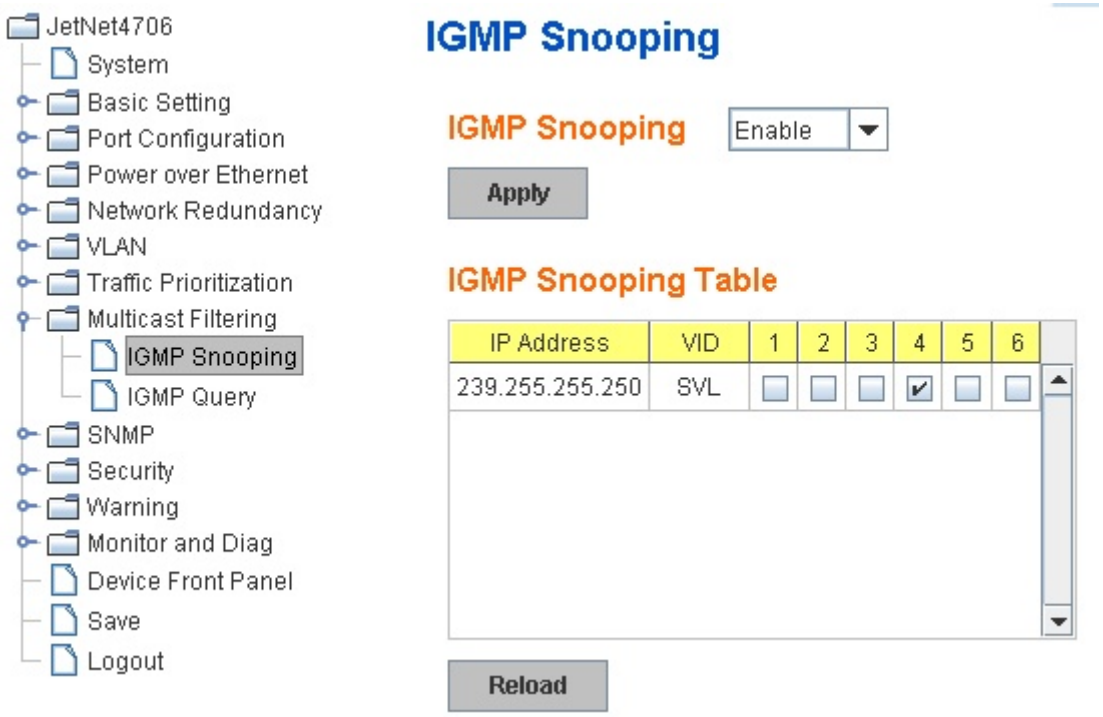
Message	Description
Query	A message sent from the querier (an IGMP router or a switch) which asks for a response from each host that belongs to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit as a member of a specific multicast group.

You can enable **IGMP Snooping** and **IGMP Query** functions here. You will see the information of the IGMP Snooping function in this section, including different multicast member ports and IP multicast addresses that range from 224.0.0.0 to 239.255.255.255.

3.7.1. IGMP Snooping

This page is to enable/disable the IGMP Snooping feature and view the IGMP

Snooping table from dynamic learnt.



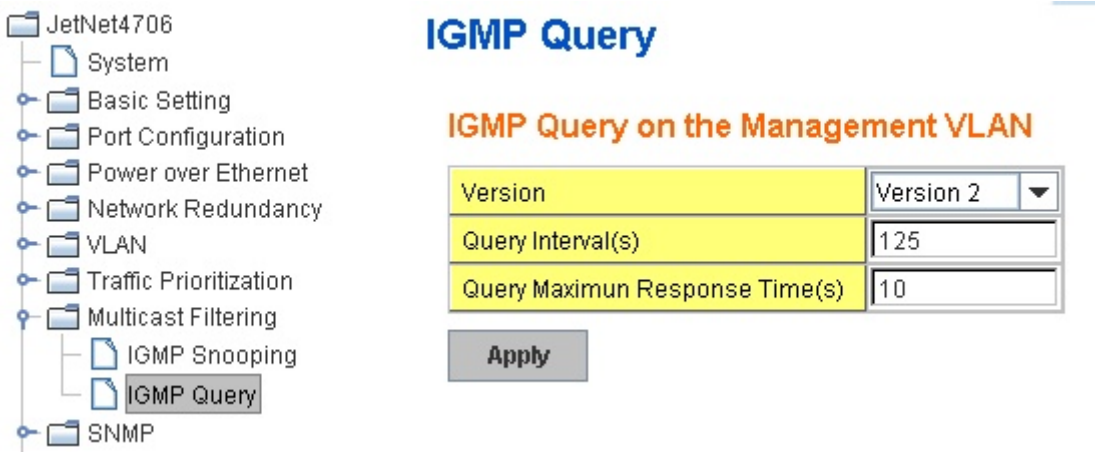
IGMP Snooping Enable / Disable IGMP snooping

IGMP Snooping Table In the table, you can see the multicast group address and the member ports of the multicast group. The switch supports 256 multicast groups. Click the **Reload** button to refresh the table.

3.7.2. IGMP Query

This page allows user to configure the **IGMP Query** feature. Since IGMP Query can only be enabled on the management VLAN. If you want to run IGMP Snooping feature in several VLANs, you should notice that whether each VLAN have their own IGMP Querier.

The IGMP querier periodically sends query packets to all end-stations on the LANs or VLANs that are connected to it. For networks with more than one IGMP querier, a switch with the lowest IP address becomes the IGMP querier.



In the IGMP Query selection, you can select V1, V2 or Disable.

V1 means IGMP V1 General Query. The query will be forwarded to all multicast groups in the VLAN.

V2 means IGMP V2 Specific Query. The query will be forwarded to specific multicast groups.

Disable disable the IGMP Query.

Once you finish configuring the settings, click the **Apply** button to apply your configuration.

3.7.3. CLI Commands of the Multicast Filtering

Feature	Command Line
IGMP Snooping	
IGMP Snooping - Global	Switch(config)# ip igmp snooping IGMP snooping is enabled globally. Please specify on which vlans IGMP snooping enables
Disable IGMP Snooping - Global	Switch(config)# no ip igmp snooping IGMP snooping is disabled globally ok.
Display – IGMP Snooping Setting	Switch# sh ip igmp snooping IGMP snooping is globally enabled
Display – IGMP Table	Switch# sh ip igmp snooping multicast all VLAN IP Address Type Ports SVL 239.192.8.0 IGMP fa6, SVL 239.255.255.250 IGMP fa6,
IGMP Query	
IGMP Query V1	Switch(config)# int vlan 1 (Go to management VLAN)

	Switch(config-if)# ip igmp v1
IGMP Query V2	Switch(config)# int vlan 1 (Go to management VLAN) Switch(config-if)# ip igmp
IGMP Query version	Switch(config-if)# ip igmp version 1 Switch(config-if)# ip igmp version 2

IGMP Query Interval	Switch(config)# int vlan 1 (Go to management VLAN)
	Switch(config-if)# ip igmp
	Switch(config-if)# ip igmp query-interval 60 (Change query interval to 60 seconds, default value is 125 seconds)

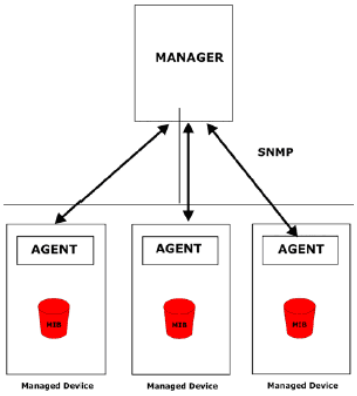
IGMP Query Max Response Time	Switch(config)# int vlan 1 (Go to management VLAN)
	Switch(config-if)# ip igmp
	Switch(config-if)# ip igmp query-max-response-time 15 (Change query max response time to 15 seconds, default value is 10 seconds)

Disable	Switch(config)# int vlan 1 Switch(config-if)# no ip igmp
Display	Switch# sh ip igmp interface vlan1 enabled: Yes version: IGMPv2 query-interval: 125s query-max-response-time: 10s Switch# show running-config .... ! interface vlan1 ip address 192.168.10.17/24 ip igmp no shutdown ! .....

3.8. SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. SNMP v1, v2c and v3 are supported.

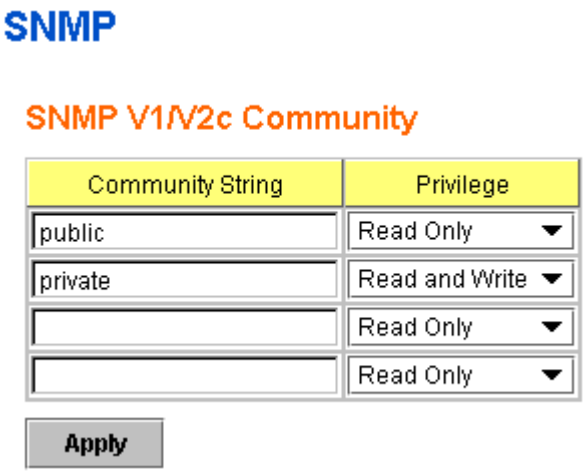
A SNMP managed network consists of two main components: agents and a manager. An agent is a management software module that resides in a managed switch. An agent translates the local management information from the managed device into a SNMP-compatible format. The manager is the console through the network.



3.8.1. SNMP Configuration

This allows users to configure the SNMP V1/ V2c Community. The community string can be treated as a password because SNMP V1/ V2c does not request you to enter a password before accessing the SNMP agent.

The community includes 2 privileges: Read Only, and Read/Write. With Read Only privileges, you will only have the ability to read the values in the MIB tables. The default community string is set to Public. With Read and Write privileges, you will have the ability to read and set the values in the MIB tables. The default community string is set to Private.



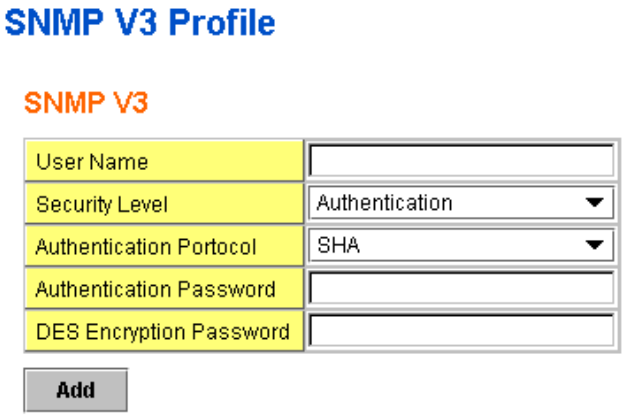
The switch supports up to 4 community strings. Enter the community string and select its privilege. Then press the Apply button.

Note: When you first install the device onto your network, we highly recommend that you change the community string. Because most SNMP management applications use Public and Private as their default community name, this may cause a leak in network security.

3.8.2. SNMP v3 Profile

SNMP v3 provides more secure functions when the user performs remote

management. It delivers SNMP information to the administrator with user's authentication. All information are encrypted to ensure a secure communication.

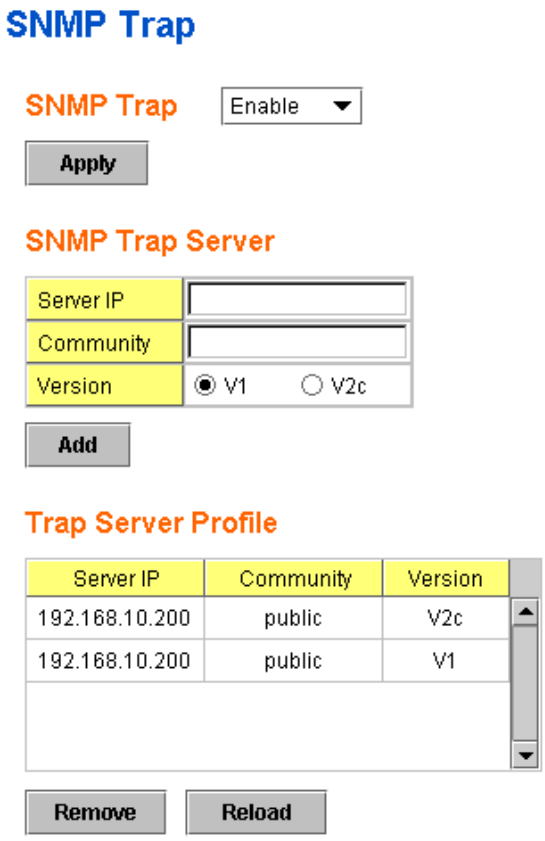


User Name	An user of SNMP v3
Security Level	Select the following levels of security: None, User Authentication, and Authentication with privacy.
Authentication Protocol	Select the authentication protocol, either MD5 (Message-Digest algorithm 5) or SHA (Secure Hash Algorithm). MD5 is a widely used cryptographic hash function with a 128-bit hash value. SHA (Secure Hash Algorithm) hash functions refer to five Federal Information Processing Standard-approved algorithms for computing a condensed digital representation. You need to configure SNMP v3 parameters for your SNMP tool with the same authentication method.
Authentication Password	The SNMP v3 user authentication password
DES Encryption Password	The password of SNMP v3 user DES Encryption

3.8.3. SNMP Traps

SNMP Trap is a notification feature defined in SNMP protocol. All SNMP management applications can understand this type of trap information.

This page allows users to **Enable SNMP Trap,** configure the **SNMP Trap server IP**, **Community** name, and trap **Version V1 or V2**. After configuration, you will be able to receive the events defined in the SNMP standard traps and Korenix private traps. The private traps can be found in Korenix's private MIB.



3.8.4. CLI Commands for SNMP

Feature	Command Line
SNMP Community	
Read Only Community	Switch(config)# snmp-server community public ro community string add ok
Read Write Community	Switch(config)# snmp-server community private rw community string add ok
SNMP Trap	
Enable Trap	Switch(config)# snmp-server enable trap Set SNMP trap enable ok.
SNMP Trap Server IP without specific community name	Switch(config)# snmp-server host 192.168.10.33 SNMP trap host add OK.
SNMP Trap Server IP with version 1 and community	Switch(config)# snmp-server host 192.168.10.33 version 1 private SNMP trap host add OK. *Note: private is the community name, version 1 is the SNMP version*
SNMP Trap Server IP with	Switch(config)# snmp-server host 192.168.10.33 version 2

version 2 and community	private SNMP trap host add OK.
Disable SNMP Trap	Switch(config)# no snmp-server enable trap Set SNMP trap disable ok.
Display	Switch# sh snmp-server trap SNMP trap: Enabled SNMP trap community: public Switch# show running-config ..... snmp-server community public ro snmp-server community private rw snmp-server enable trap snmp-server host 192.168.10.33 version 2 admin snmp-server host 192.168.10.33 version 1 admin .....

3.9. Security

By IP Security, you are able to set up specific IP addresses to perform authorization for management access to the switch via web browser, Telnet or SNMP.

Once you have finished configuring the settings, click the **Apply** button to apply your configuration.

3.9.1. IP Security

Add Security IP You can assign any PC as an authenticated workstation by adding a PC's IP address into the Security IP field. Only these IP addresses will be able to access and manage the switch. The maximum number of security IP is 10.

Security IP List This table shows you each security IP address you have added. You can hit **Remove** to delete, and **Reload** to reload the table.

Once you have finished configuring the settings, click the **Apply** buttonto apply your configuration.

3.9.2. CLI Commands for Security

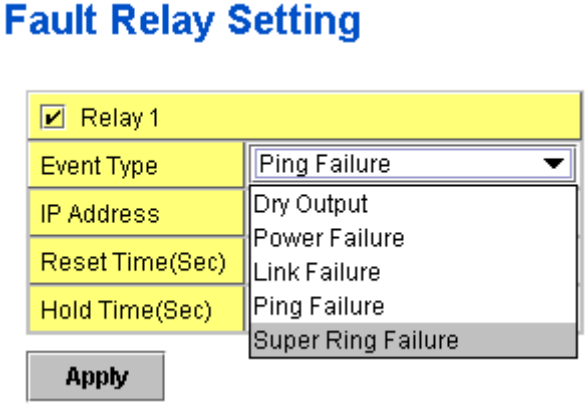
Feature	Command Line
IP Security	
IP Security	Switch(config)# ip security Set ip security enable ok. Switch(config)# ip security host 192.168.10.33 Add ip security host 192.168.10.33 ok.
Display	Switch# show ip security ip security is enabled ip security host: 192.168.10.33

3.10. Warning

This switch provides several types of warning features for remote monitoring and a real-time alert mechanism. These features include a System Log for local and remote servers, SMTP E-mail alerts and a Fault Relay alarm.

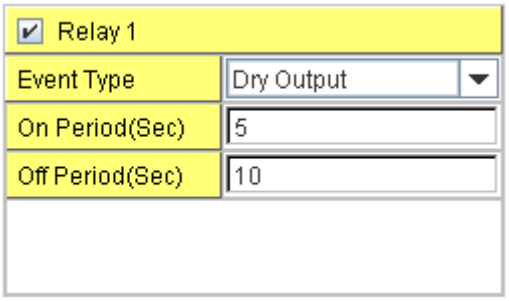
3.10.1. Fault Relay Setting

This device provides 1 digital output, also known as Relay Output. The relay contacts are energized (open) for normal operation and will close under faulty conditions. Faulty conditions include Power Failure, Ethernet port Link Failure, Ping Failure and Super Ring Topology Change. You can enable and select relay trigger by clicking the **Apply** button.



Relay 1 Check the box **Relay 1** and then select the Event Type and its parameters.

Event Type You will be given the following options: Dry Output, Power Failure, Link Failure, Ping Failure and Super Ring Failure. Each event type has its own parameters. A Relay can be related one event type, detailed below

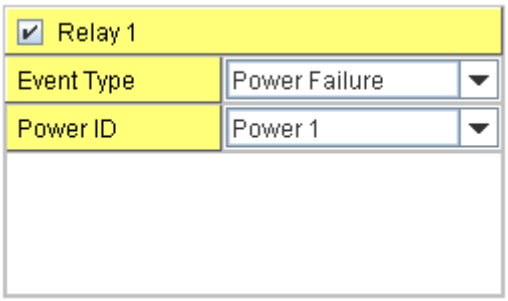


Dry Output

On Period (Sec) Type in the amount of time you would like Relay Output to be on. This can range from 0-4294967295 seconds.

Off Period (Sec) Type in the amount of time you would like Relay Output to be off. This can range from 0-4294967295 seconds.

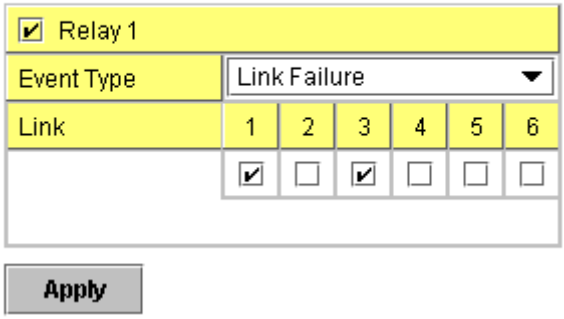
When the amount of time is reached, the system will turn the Relay Output on or off.



Power Failure

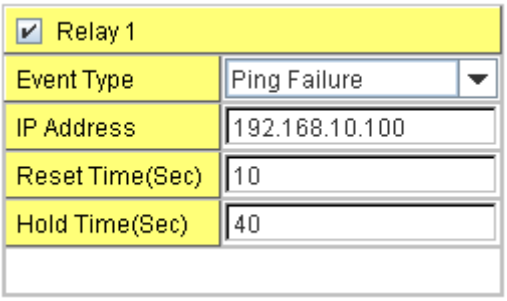
Power ID Select either Power 1 or Power 2. When power is shut down, the system will short Relay Out and light the DO LED.

Fault Relay Setting



Link Failure

Link Select the port ID you would like to monitor. Check the box of the Ethernet ports you wish to monitor. You may select multiple ports. When the selected ports are unlinked, the system will short Relay Output and light the DO LED.



Ping Failure

IP Address: Enter the IP address of the target device you want to ping.

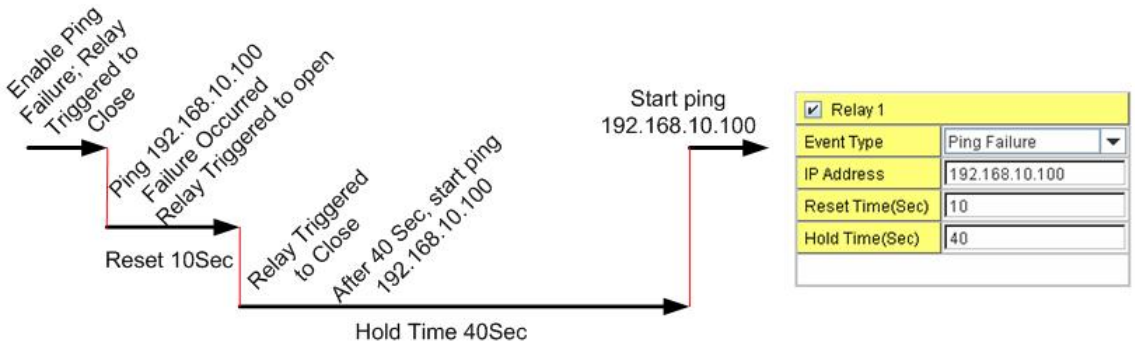
Reset Time (Sec) Enter the amount of time after ping has failed that you would like the relay output to turn off

Hold Time (Sec) Enter the amount of time after ping has failed and relay output has been turned off, that you would like the relay output to be turned back on.

After selecting the Ping Failure event type, the system will change the Relay Output to “short” state, light the alarm LED and continuously ping the target device. When the ping failure for Reset Time times out, the system will change the Relay Output to “open” state and turn off the alarm LED for the amount of time entered in **Hold Time**. After the Hold Time times out, the system will start sending ping commands to the remote device.

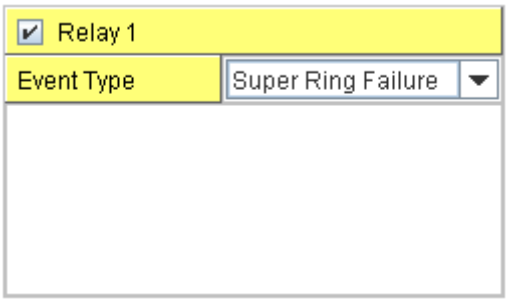
For example, the **Reset Time** is set to 10 sec and the **Hold Time** is set to 40 sec. The system will turn the Relay Output and Alarm LED off after ping has failed for 10 seconds (Reset Time). The system will turn the Relay Output and alarm LED on again after 40 seconds (Hold Time).

The change of state of a Relay Output Ping Failure Event, see the chart below.



Super Ring Failure

Select Super Ring Failure. When the Rapid Super Ring topology is changed, the system will short Relay Out and light the alarm LED.



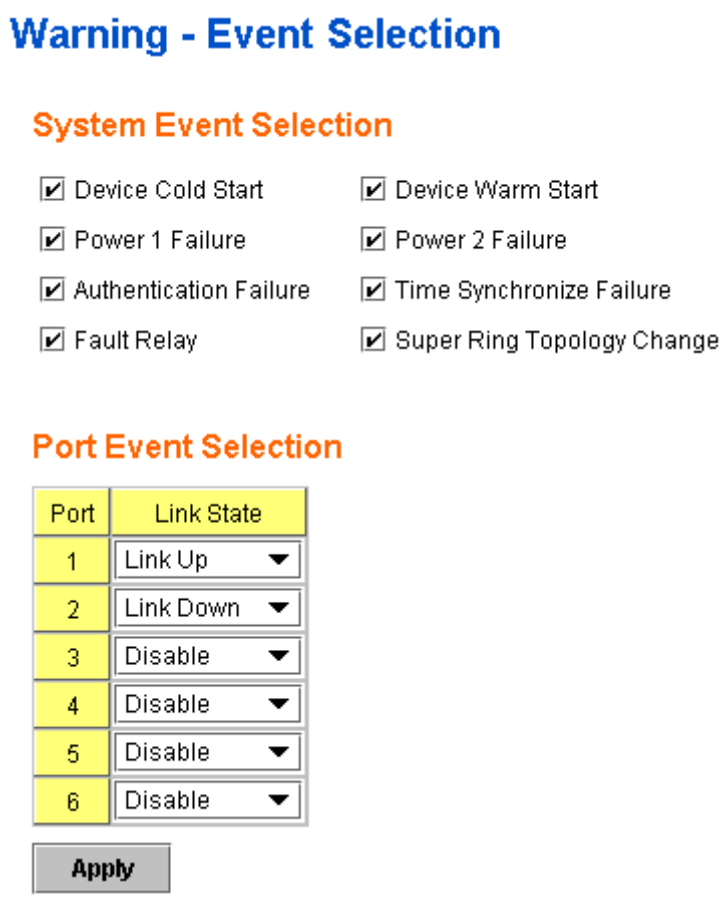
Once you have finished configuring the settings, click the **Apply** button to apply your configuration.

3.10.2. Event Selection

Event Types are divided into 2 basic groups: System Events and Port Events. System Events relate to the overall function of the switch whereas Port Events

relate to the activity of specific ports.

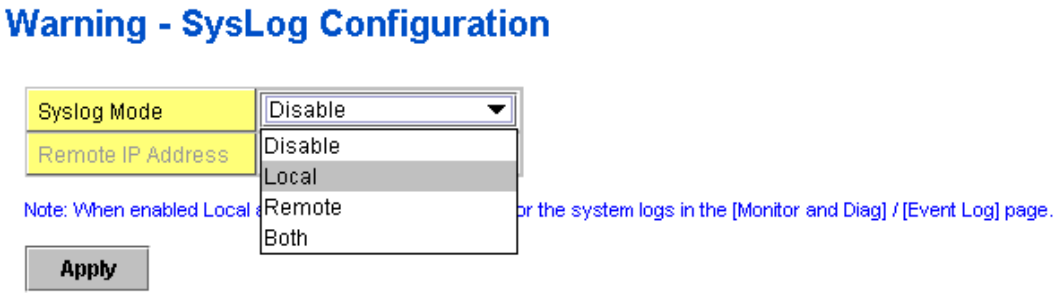
System Event	Warning Event is sent when.....
Device Cold Start	Power is cut off and then reconnected.
Device Warm Start	Reboot the device by CLI or Web UI.
Power 1 Failure	Power 1 is failure.
Power 2 Failure	Power 2 is failure.
Authentication failure	An incorrect password, SNMP Community String is entered.
Time Synchronize Failure	Time Synchronize Failure
Fault Relay	The DO/Fault Relay is on.
Super Ring Topology Changes	Master of Super Ring has changed or backup path is activated.
Port Event	**Warning Event is sent when.....**
Link-Up	The port is connected to another device
Link-Down	The port is disconnected (e.g. the cable is pulled out, or the opposing devices turns down)



Once you have finished configuring the settings, click the Apply buttonto apply your configuration.

3.10.3. SysLog Configuration

System Log is useful in providing the system administrator both local and remote monitoring of the switch's history. There are 3 System Log modes, local, remote and both.



Local In this mode, the device will print selected past events (selected in the Event Selection page) to the System Log table. You can monitor the system logs in the [Monitor and Diag] / [Event Log] page.

Remote The remote mode is also known as Server mode. In this mode, you should assign the IP address of the System Log server. The device will send the selected occurrences, selected on the Event Selection page, to the System Log server that you have assigned.

Both The 2 modes mentioned above can be enabled at the same time.

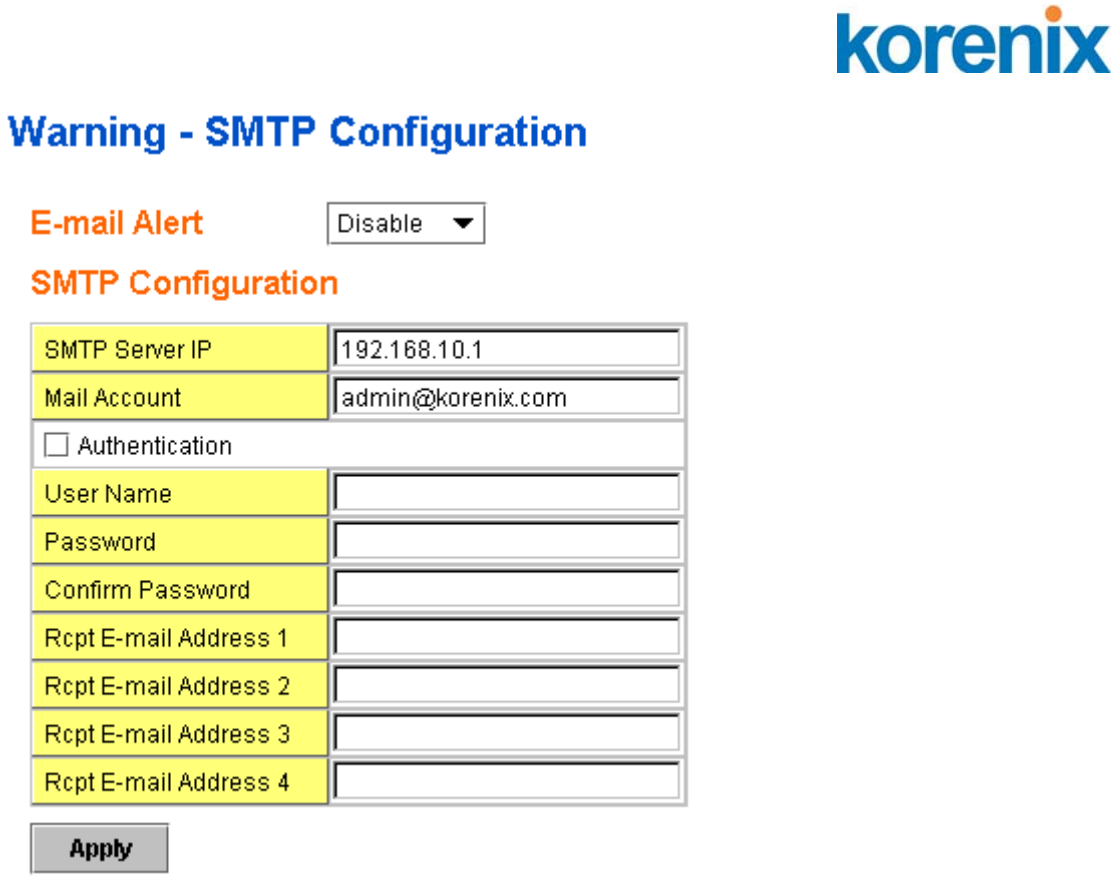
When enabling Local or Both modes, you can monitor the system logs in [Monitor and Diag] / [Event Log] page.

Once you have finished configuring the settings, click the **Apply** button to apply your configuration.

3.10.4. SMTP Configuration

The switch includes an E-mail Warning feature. The switch will send event warnings to a remote E-mail server. The receiver can then receive an E-mail notification by according to SMTP standards.

The web page allows you to enable the E-mail Alert, and assign the SMTP Server IP, Sender E-mail, and Receiver E-mail. Enter the username and password if authorization is required to login the SMTP server.



SMTP Server IP Address Enter the IP address of the email Server

Authentication Click the check box to enable password

User Name Enter email Account name (Max.40 characters)

Password Enter the password of the email account

Confirm Password Re-type the password of the email account

You can set up to 4 email addresses to receive email alarm

Rcpt E-mail Address 1 The first email address to receive email alert (Max. 40 characters)

Rcpt E-mail Address 2 The second email address to receive email alert (Max. 40 characters)

Rcpt E-mail Address 3 The third email address to receive email alert (Max. 40 characters)

Rcpt E-mail Address 4 The fourth email address to receive email alert (Max. 40 characters)

Once you have finished configuring the settings, click the Apply button to apply your configuration.

3.10.5. CLI Commands for Warning

Feature	Command Line
Relay Output	

Relay Output	Switch(config)# relay 1 dry dry output ping ping failure port port link failure power power failure ring super ring failure
Dry Output	Switch(config)# relay 1 dry <0-4294967295> turn on period in second Switch(config)# relay 1 dry 5 <0-4294967295> turn off period in second Switch(config)# relay 1 dry 5 5
Ping Failure	Switch(config)# relay 1 ping 192.168.10.33 <cr> reset reset a device Switch(config)# relay 1 ping 192.168.10.33 reset <1-65535> reset time Switch(config)# relay 1 ping 192.168.10.33 reset 60 <0-65535> hold time to retry Switch(config)# relay 1 ping 192.168.10.33 reset 60 60
Port Link Failure	Switch(config)# relay 1 port PORTLIST port list Switch(config)# relay 1 port fa1-5
Power Failure	Switch(config)# relay 1 power <1-2> power id Switch(config)# relay 1 power 1 Switch(config)# relay 1 power 2
Super Ring Failure	Switch(config)# relay 1 ring
Disable Relay	Switch(config)# no relay <1-2> relay id Switch(config)# no relay 1 *(Relay_ID: 1 or 2)* <cr>
Display	Switch# show relay 1 Relay Output Type : Port Link Port : 1, 2, 3, 4, Switch# show relay 2 Relay Output Type : Super Ring
Event Selection	
Event Selection	Switch(config)# warning-event

	coldstart Switch cold start event warmstart Switch warm start event linkdown Switch link down event linkup Switch link up event all Switch all event authentication Authentication failure event fault-relay Switch fault relay event power Switch power failure event super-ring Switch super ring topology change event time-sync Switch time synchronize failure event
Ex: Cold Start event	Switch(config)# warning-event coldstart Set cold start event enable ok.
Ex: Link Up event	Switch(config)# warning-event linkup [IFNAME] Interface name, ex: fastethernet1 or gi8 Switch(config)# warning-event linkup fa5 Set fa5 link up event enable ok.
Display	Switch# show warning-event Warning Event: Cold Start: Enabled Warm Start: Disabled Authentication Failure: Disabled Link Down: fa4-5 Link Up: fa4-5 Power Failure: Super Ring Topology Change: Disabled Fault Relay: Disabled
Syslog Configuration	
Local Mode	Switch(config)# log syslog local
Server Mode	Switch(config)# log syslog remote 192.168.10.33
Both	Switch(config)# log syslog local Switch(config)# log syslog remote 192.168.10.33
Disable	Switch(config)# no log syslog local
SMTP Configuration	
SMTP Enable	Switch(config)# smtp-server enable email-alert SMTP Email Alert set enable ok.
Sender mail	Switch(config)# smtp-server server 192.168.10.100 ACCOUNT SMTP server mail account, ex: admin@korenix.com

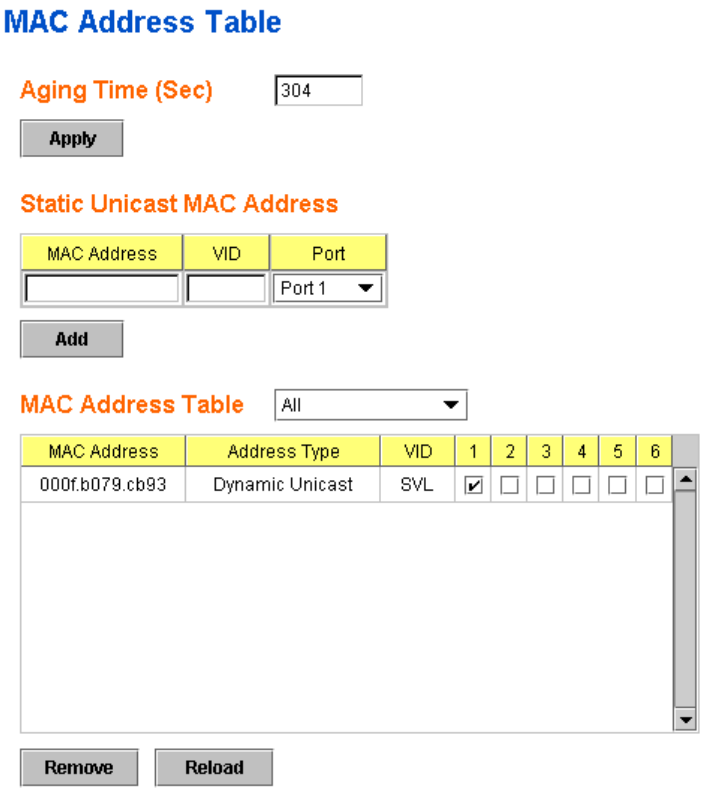
	Switch(config)# smtp-server server 192.168.10.100 admin@korenix.com SMTP Email Alert set Server: 192.168.10.100, Account: admin@korenix.com ok.
Receiver mail	Switch(config)# smtp-server receipt 1 korecare@korenix.com SMTP Email Alert set receipt 1: korecare@korenix.com ok.
Authentication with username and password	Switch(config)# smtp-server authentication username admin password admin SMTP Email Alert set authentication Username: admin, Password: admin Note: You can assign string to username and password.
Disable SMTP	Switch(config)# no smtp-server enable email-alert SMTP Email Alert set disable ok.
Disable Authentication	Switch(config)# no smtp-server authentication SMTP Email Alert set Authentication disable ok.
Dispaly	Switch# sh smtp-server SMTP Email Alert is Enabled Server: 192.168.10.100, Account: admin@korenix.com Authentication: Enabled Username: admin, Password: admin SMTP Email Alert Receipt: Receipt 1: korecare@korenix.com Receipt 2: Receipt 3: Receipt 4:

3.11. Monitoring and Diagnostic

There are several types of features for monitoring the switch's status or create a diagnostic to check if any problems occur. The features include MAC Address Table, Port Statistics, Port Mirror, Event Log and Ping.

3.11.1. MAC Address Table

There are 2K entries in the MAC Address Table. On this page, you can change Aging Time, add Static Unicast MAC Address, monitor the MAC address or sort them by different packet types and ports.



Aging Time (Sec)

Each switch fabric has a limited amount of space to write the learnt MAC address. To save more entries for new MAC address, the switch fabric will age out any unused MAC address entries with respect to the Aging Time. The default Aging Time is 300 seconds. The Aging Time can be modified on this page.

Static Unicast MAC Address

For some applications, users may need to type the static Unicast MAC address into its MAC address table. On this page, you can type in the MAC Address (format: xxxx.xxxx.xxxx), and select its VID and Port ID. Click the **Add** buttonto add it to the MAC Address table.

MAC Address Table

In the MAC Address Table, you can see all the MAC Addresses learned by the switch fabric. The packet types include Management Unicast, Static Unicast, Dynamic Unicast, Static Multicast and Dynamic Multicast. The table allows users to sort the addresses by the packet types and the port.

Management Unicast refers to the MAC address

of the switch. It belongs to the CPU port only. **Static Unicast** MAC address can be added and deleted. **Dynamic Unicast** MAC is the MAC address learned by the switch Fabric. **Static Multicast** can be added through CLI and can be deleted through the Web and CLI. **Dynamic Multicast** will appear after you have enabled IGMP and after the switch learns the IGMP report.

Click the **Remove** button to remove the Static Unicast/Multicast MAC address. Click the **Reload** buttonto refresh the table. Newly learned Unicast/Multicast MAC addresss will be updated to the MAC address table.

Click the **Apply** button to change the value.

3.11.2. Port Statistics

This page summarizes the operational statistics for each port. The statistics include Link Type, Link State, Rx Good, Rx Bad, Tx Good, and Collision. Rx means the received packets while Tx means the transmitted packets. The statistics can just show Rx Good and Tx Good or Rx Bad and Collision.

Note: If you see an increase in Bad or Collision counts, this may mean that your network cable is not connected correctly or the network performance of the port is poor. Please check your network cable, Network Interface Card connected to your device, the network application, or reallocate the network traffic.

Port Statistics

Port	Type	Link	State	Rx Good	Rx Bad	Tx Good	Collision
1	100BASE	Down	Enable	0	--	0	--
2	100BASE	Down	Enable	0	--	0	--
3	100BASE	Down	Enable	0	--	0	--
4	100BASE	Down	Enable	0	--	0	--
5	100BASE	Down	Enable	0	--	0	--
6	100BASE-TX	Up	Enable	212	--	230	--

Clear All | Reload | Bad-Collision Mode

Clear All reset the counts of all ports

Reload refresh the counts

Bad-Collision Mode change to Rx Bad and Tx Collisions mode and the

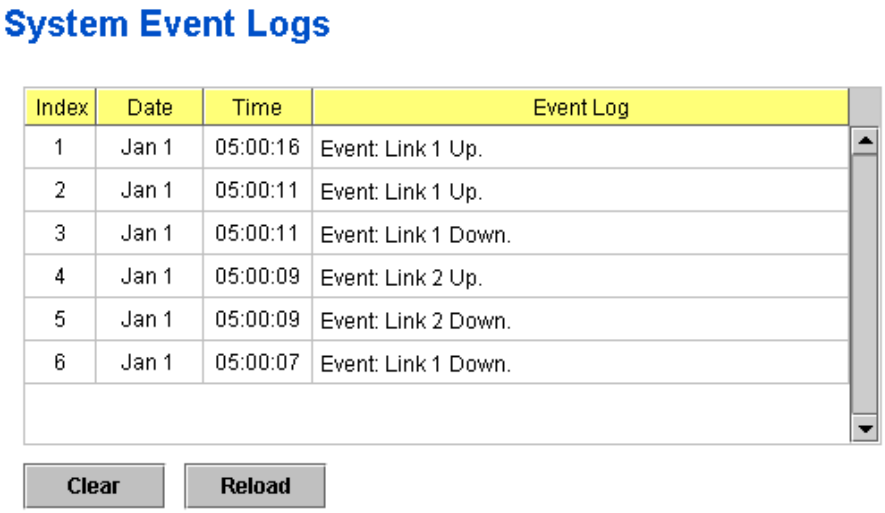
Good Mode change to Rx Good and Tx Good mode.

Note: If the mode is changed. The statistics counter will be reset to 0

3.11.3. Event Log

When Local mode of System Log is selected, the switch records events in the local log table. This page shows the log table. The entries include the index, and data, time and content of the occurrences.

Click the **Clear** button to delete the entries. Click the **Reload** button to refresh the table.


System Event Logs
Index
Date
Time
Event Log
1 Jan 1 05:00:16 Event: Link 1 Up.
2 Jan 1 05:00:11 Event: Link 1 Up.
3 Jan 1 05:00:11 Event: Link 1 Down.
4 Jan 1 05:00:09 Event: Link 2 Up.
5 Jan 1 05:00:09 Event: Link 2 Down.
6 Jan 1 05:00:07 Event: Link 1 Down.
Clear
Reload

3.11.4. Ping Utility

This page provides **Ping Utility** for users to ping remote devices and to check whether the device is alive or not. Type the target IP address of the target device into **Target IP.** Click the **Start** button to start the ping. You will be able to see the results in the **Result** field.

Ping Utility

Ping

Target IP 192.168.10.200

Start

Result

```
PING 192.168.10.200 (192.168.10.200): 56 data bytes
64 bytes from 192.168.10.200: icmp_seq=0 ttl=128 time=0.0 ms
64 bytes from 192.168.10.200: icmp_seq=1 ttl=128 time=0.0 ms
64 bytes from 192.168.10.200: icmp_seq=2 ttl=128 time=0.0 ms
64 bytes from 192.168.10.200: icmp_seq=3 ttl=128 time=0.0 ms
64 bytes from 192.168.10.200: icmp_seq=4 ttl=128 time=0.0 ms

--- 192.168.10.200 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

3.11.5. CLI Commands for Monitoring and Diagnostic

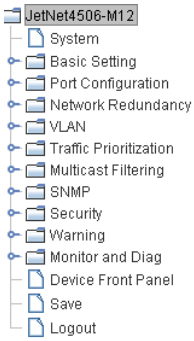
Feature	Command Line
MAC Address Table	
Ageing Time	Switch(config)# mac-address-table aging-time 350 mac-address-table aging-time set ok! *Note: 350 is the new ageing timeout value.*
Add Static Unicast MAC address	Switch(config)# mac-address-table static 0012.7701.0101 vlan 1 interface fastethernet1 mac-address-table ucast static set ok! *Note: rule: mac-address-table static MAC_address VLAN VID interface interface_name*
Add Multicast MAC address	Switch(config)# mac-address-table multicast 0100.5e01.0101 vlan 1 interface fa1-6 Adds an entry in the multicast table ok! *Note: rule: mac-address-table multicast MAC_address VLAN VID interface_list interface_name/range*
Show MAC Address Table – All types	Switch# show mac-address-table ***** UNICAST MAC ADDRESS ***** Destination Address Address Type Vlan Destination Port ——————— ——————— ——— ——————— 000f.b079.ca3b Dynamic 1 fa1 0012.7701.0386 Dynamic 1 fa2 0012.7710.0101 Static 1 fa6 0012.7710.0102 Static 1 fa6 0012.77ff.0100 Management 1 ***** MULTICAST MAC ADDRESS *****

	Vlan Mac Address COS Status Ports — ———— — ——— ———— 1 0100.5e40.0800 0 fa6 1 0100.5e7f.fffa 0 fa4,fa6
Show MAC Address Table – Dynamic Learnt MAC addresses	Switch# show mac-address-table dy Destination Address Address Type Vlan Destination Port ———— ———— — ———— 000f.b079.cb93 Dynamic SVL fa1
Show MAC Address Table – Multicast MAC addresses	Switch# show mac-address-table multicast Switch# show mac-address-table multicast Vlan Mac Address COS Status Ports — ———— — ——— ————
Show MAC Address Table – Static MAC addresses	Switch# show mac-address-table static Destination Address Address Type Vlan Destination Port ———— ———— ——— ———— 0012.7710.0101 Static 1 fa6 0012.7710.0102 Static 1 fa6
Show Aging timeout time	Switch# show mac-address-table aging-time the mac-address-table aging-time is 304 sec.

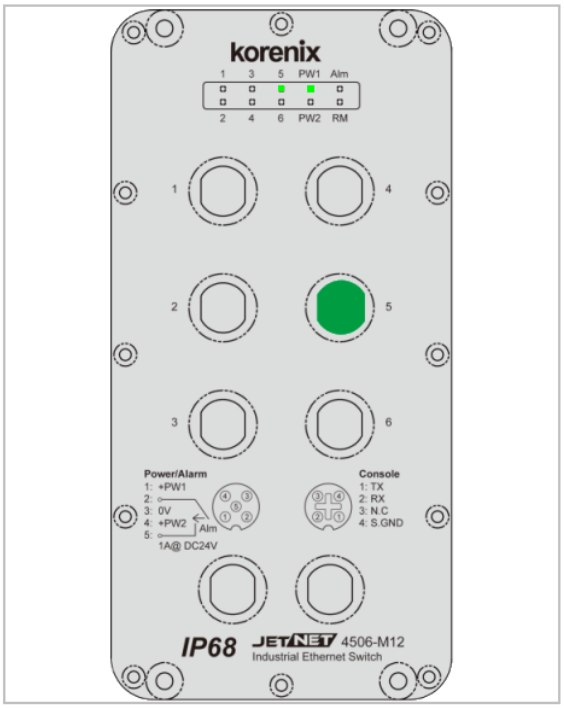
Port Statistics	
Port Statistics	Switch# show rmon statistics fa4 (select interface) RMON statistics counter mode is RxGood and TxGood mode. Interface fastethernet1 is enable connected, which has Inbound: RxGood: 1292 Outbound: TxGood: 1978
Bad-Collision Mode	Switch(config)# rmon statistics counter-mode error-collisions Set RMON statistics counter mode to RxError and TxCollisions mode.
Good Mode	Switch(config)# rmon statistics counter-mode good Set RMON statistics counter mode to RxGood and TxGood mode.
Event Log	
Display	Switch# show event-log <1>Jan 1 02:50:47 snmpd[101]: Event: Link 4 Down. <2>Jan 1 02:50:50 snmpd[101]: Event: Link 5 Up. <3>Jan 1 02:50:51 snmpd[101]: Event: Link 5 Down. <4>Jan 1 02:50:53 snmpd[101]: Event: Link 4 Up.
Ping	
Ping IP	Switch# ping 192.168.10.33 PING 192.168.10.33 (192.168.10.33): 56 data bytes 64 bytes from 192.168.10.33: icmp_seq=0 ttl=128 time=0.0 ms 64 bytes from 192.168.10.33: icmp_seq=1 ttl=128 time=0.0 ms 64 bytes from 192.168.10.33: icmp_seq=2 ttl=128 time=0.0 ms 64 bytes from 192.168.10.33: icmp_seq=3 ttl=128 time=0.0 ms 64 bytes from 192.168.10.33: icmp_seq=4 ttl=128 time=0.0 ms — 192.168.10.33 ping statistics — 5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms

3.12. Device Front Panel

Device Front Panel displays the LED panel which indicates status of power and link status.

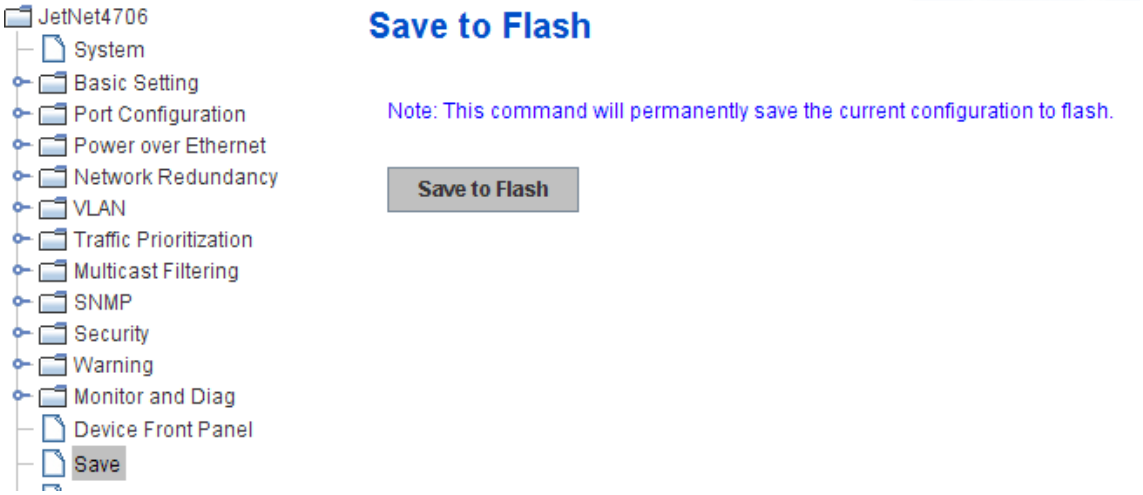


Device Front Panel



3.13. Save to Flash

Save Configuration allows you to save any configuration you just made to the Flash. Powering off the switch without clicking Save Configuration will cause loss of new settings. After selecting Save Configuration, click the **Save to Flash** button to save your new configuration.

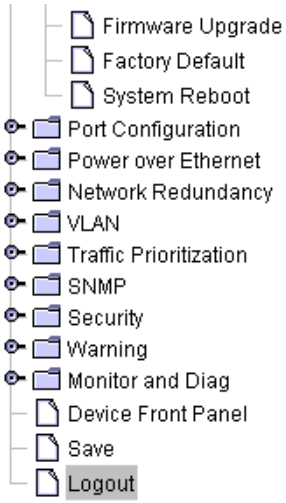


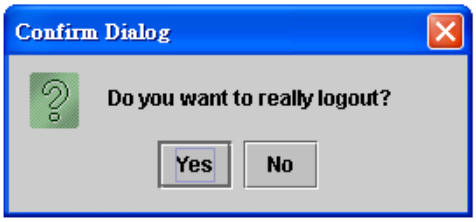
3.13.1. CLI Commands for Save to Flash

Feature	Command Line
Save	Switch# write Building Configuration... [OK] Switch# copy running-config startup-config Building Configuration... [OK]

3.14. Logout

The switch provides 2 logout methods. Your web connection will log out if you do not input a command for 30 seconds. The Logout command allows you to manually log out the web connection. Click **Yes** to logout, and **No** to go back to the configuration page.





3.14.1. CLI Commands for Logout

Feature	Command Line
Logout	Switch> exit Switch# exit

Appendix A. Korenix Private MIB

Korenix supports standard MIBs to configure or monitor the switch for common features. In addition, Korenix provides privates MIB which includes both the features of standard MIBs and all the proprietary functions. For your convenience, the structure of the private MIB is designed to be the same as the structure of web interface. With the private MIB, you can configure the device through SNMP very easily.

Find private MIBs in the product CD or download from the Korenix Web site www.korenix.com.

Appendix B. Technical Data

B.1. JetNet 4506-RJ

Technology

Standard:

IEEE 802.3 10Base-T

IEEE 802.3u 100Base-TX

IEEE 802.1p Class of Service

IEEE 802.3x Flow Control and Back-pressure

IEEE 802.1D Spanning Tree

IEEE 802.1w Rapid Spanning Tree

Performance

Switch Technology:

Store and Forward Technology with 3.2Gbps wire-speed non-blocking Switch Fabric

System Throughput: 1.785Mpps

MAC Address: 2000

Packet Buffer: Embedded 1Mbits shared buffer

Transfer performance: 14,880pps for Ethernet and 148,810pps for Fast Ethernet

Transfer packet size: from 64 to 1536Bytes

Relay Alarm: Dry Relay output with 1A @ 24V

Management

Management Interface: SNMP v1, v2c and v3, Web browser, JetView and CLI Management

Management Security: 4 entries for web, telnet, SNMP management security

SNMP Trap: Provides Cold start, Warm start, Port event, Power event, Authentication failure, and Korenix private trap for proprietary functions

SNMP MIB: RFC 1213 MIBII, RFC 1493 Bridge MIB, RFC 1757 RMON MIB, RFC 2674 VLAN MIB, RFC 1643 Ethernet like MIB, RFC1215 Trap MIB, Korenix Private MIB

Firmware upgrade: TFTP, Local file and JetView

System Log: 1000 system entries for system or remote log server

Event Alarm Relay: 1A @24V Dry Relay Contact output for Super Ring failure, port link down, System power events.

Quality of Service: Quality of Service determined by port, Tag or IPv4 Type of Service

Class of Service: IEEE802.1p class of service, with 4 priority queues

DHCP: Supports DHCP Cilent, DHCP Agent with Option 82, DHCP Server specified IP exclusion and MAC binding function

Timer: Supports Network Time Protocol (NTP) to synchronize time from NTP Server

VLAN: Port based VLAN

IGMP Snooping: Supports IGMP Snooping v1/v2/v3 and IGMP Query v1/v2

Network Redundancy: Supports Rapid Super Ring function for network redundancy with 5ms network recovery time. To inter-operate with other higher level switches, JetNet 4506-RJ provides Rapid Dual Homing technology.

JetNet 4506-RJ also conforms to IEEE802.1D 2004 edition for RSTP and STP standard protocols

IP Security: IP security to prevent unauthorized access

Interface

Number of Ports:

6 x 10/100Base-TX ports

1 x RS-232 Console

1 x Redundant Power with Relay Alarm

Connectors:

10/100TX: Rugged RJ45

RS-232 Console: M12 A-coding 4-ping socket

Power: M12 A-coding 5-pin socket

Cable:

10Base-T: 4-pair UTP/STP Cat. 4, 5 cable,

100Base-TX: 4-pair UTP/STP Cat.5,

Cat.5E/Cat.6 cable,

Diagnostic LED:

PW1/PW2: Power on (Green)

Fast Ethernet: Link (Green) / Activity (Green blinking),

Alm: Relay Alarm for Super Ring failure, port link down or power failure occurred (Red)

RM: Ring Manager (Green)

Power Requirements

Power Consumption:

Operating Voltage: 12 to 48V DC

Power consumption: max 10 Watts @ 48V

Mechanical

Protection class: IP67

Installation: Wall mount

Case: Aluminum metal case

Dimension: 213.6 mm (H) x 106.0 mm (W) x 56.5 mm (D)

Weight:1090 g without package

Environmental

Operating Temperature: -25 ~ 70OC

Storage Temperature: -40 ~ 85OC

Regulatory Approvals

DNV: pending

EN 50155 Railway: compliance

Safety: CE/EN60950(Pending)

EMI:

FCC Class A; CE/EN55022:2003 Class A;

CE/EN61000-3-2:2001 Harmonic Test;

CE/EN61000-3-3:1995 Flicker test

EMS:

EN61000-4-2:1998,ESD

EN61000-4-3:1998, RS

EN61000-4-4:1995, EFT

EN61000-4-5:1995, Surge

EN61000-4-6:1996, CS

EN61000-4-8:PFM

Shock: IEC60068-2-27

Vibration: IEC60068-2-6

Free Fall: IEC60068-2-32

B.2. JetNet 4506-M12

Technology

Standard:

IEEE 802.3 10Base-T

IEEE 802.3u 100Base-TX

IEEE 802.1p Class of Service

IEEE 802.3x Flow Control and Back-pressure

IEEE 802.1D Spanning Tree

IEEE 802.1w Rapid Spanning Tree

Performance

Switch Technology:

Store and Forward Technology with 3.2Gbps wire-speed non-blocking Switch Fabric

System Throughput: 1.785Mpps

MAC Address: 2000

Packet Buffer: Embedded 1Mbits shared buffer

Transfer performance: 14,880pps for Ethernet and 148,810pps for Fast Ethernet

Transfer packet size: from 64 to 1536Bytes

Relay Alarm: Dry Relay output with 1A @ 24V

Management

Management interface: SNMP v1, v2c and v3, Web browser, JetView and CLI Management

Management Security: 4 entries for web, telnet, SNMP management security

SNMP Trap: Provides Cold start, Warm start, Port event, Power event, Authentication failure, and Korenix private trap for proprietary functions

SNMP MIB: RFC 1213 MIBII, RFC 1493 Bridge MIB, RFC 1757 RMON MIB, RFC 2674 VLAN MIB, RFC 1643 Ethernet like MIB, RFC1215 Trap MIB, Korenix Private MIB

Firmware upgrade: TFTP, Local file and JetView

System Log: 1000 system entries for system or remote log server

Event Alarm Relay: 1A @24V Dry Relay Contact output for Super Ring failure, port link down, System power events.

Quality of Service: Quality of Service determined by port, Tag or IPv4 Type of Service

Class of Service: IEEE802.1p class of service, with 4 priority queues

DHCP: Supports DHCP Cilent, DHCP Agent with Option 82, DHCP Server specified IP exclusion and MAC binding function

Timer: Supports Network Time Protocol (NTP) to synchronize time from NTP Server

VLAN: Port based VLAN

IGMP Snooping: Supports IGMP Snooping v1/v2/v3 and IGMP Query v1/v2

Network Redundancy: Supports Rapid Super Ring function for network redundancy with 5ms network recovery time. To inter-operate with other higher level switches, JetNet 4506-M12 provides Rapid Dual Homing technology. JetNet 4506-M12 also conforms with IEEE802.1D 2004 edition for RSTP and STP standard protocols

IP Security: IP security to prevent unauthorized access

Interface

Number of Ports:

6 x 10/100Base-TX ports

1 x RS-232 Console

1 x Redundant Power with Relay Alarm

Connectors:

10/100TX: M12 D-coding 4-pin socket

RS-232 Console: M12 A-coding 4-ping socket

Power: M12 A-coding 5-pin socket

Cable:

10/100 Base-TX: 2-pair cable

Diagnostic LED:

PW1/PW2: Power on (Green)

Fast Ethernet: Link (Green) / Activity (Green blinking),

Alm: Relay Alarm for Super Ring failure port link down or power failure occurred (Red)

RM: Ring Manager (Green)

Power Requirements

Power Consumption:

Operating Voltage: 12 to 48V DC

Power consumption: max 10 Watts @ 48V

Mechanical

Protection Class: IP68

Installation: Wall mount

Case: Aluminum metal case

Dimension: 213.6 mm (H) x 106.0 mm (W) x 56.5 mm (D)

Weight: 1110 g without package

Environmental

Operating Temperature: -25 ~ 700C

Storage Temperature: -40 ~ 850C

Regulatory Approvals

DNV: pending

EN 50155 Railway: compliance

Safety: CE/EN60950

EMI:

FCC Class A; CE/EN55022:2003 Class A;

CE/EN61000-3-2:2001 Harmonic Test;

CE/EN61000-3-3:1995 Flicker test

EMS:

EN61000-4-2:1998,ESD

EN61000-4-3:1998, RS

EN61000-4-4:1995, EFT

EN61000-4-5:1995, Surge

EN61000-4-6:1996, CS

EN61000-4-8: PFM

Shock: IEC60068-2-27

Vibration: IEC60068-2-6

Free Fall: IEC60068-2-32

B.3. JetNet 3006-RJ

Technology

Standard:

IEEE 802.3 10Base-T

IEEE 802.3u 100Base-TX

IEEE 802.3x Flow Control and Back-pressure

Broadcast storm control

Performance

Switch Technology:

Store and Forward Technology with 3.2Gbps wire-speed non-blocking Switch Fabric

System Throughput: 1.785Mpps

MAC Address: 2000

Packet Buffer: Embedded 1Mbits shared buffer

Transfer performance: 14,880pps for Ethernet and 148,810pps for Fast Ethernet

Transfer packet size: from 64 to 1536Bytes

Interface

Number of Ports:

6 x 10/100Base-TX ports

Connectors:

10/100TX: Rugged RJ45

Power: M12 A-codeing 5-pin connector

Cable:

10Base-T: 4-pair UTP/STP Cat. 4, 5 cable,

100Base-TX: 4-pair UTP/STP Cat.5,

Cat.5E/Cat.6 cable,

Diagnostic LED:

Power: Power On (Green)

Fast Ethernet: Link (Green) / Activity (Green blinking),

Power Requirements

Power Consumption:

Operating Voltage: 12 to 48V DC

Power consumption: max 6 Watts @ 48V

Mechanical

Protection class: IP67

Installation: Wall mount

Case: Aluminum metal case

Dimension: 213.6 mm (H) x 106.0 mm (W) x 56.5 mm (D)

Weight:

1075 g with package

Environmental

Operating Temperature: -25 ~ 70OC

Storage Temperature: -40 ~ 85OC

Regulatory Approvals

DNV: pending

EN 50155 Railway: compliance

Safety: CE/EN60950

EMI:

FCC Class A; CE/EN55022:2003 Class A;

CE/EN61000-3-2:2001 Harmonic Test;

CE/EN61000-3-3:1995 Flicker test

EMS:

EN61000-4-2:1998,ESD

EN61000-4-3:1998, RS

EN61000-4-4:1995, EFT

EN61000-4-5:1995, Surge

EN61000-4-6:1996, CS

EN61000-4-8:PFM

Shock: IEC60068-2-27

Vibration: IEC60068-2-6

Free Fall: IEC60068-2-32

B.4. JetNet 3006-M12

Technology

Standard:

IEEE 802.3 10Base-T

IEEE 802.3u 100Base-TX

IEEE 802.3x Flow Control and Back-pressure

Broadcast storm control

Performance

Switch Technology:

Store and Forward Technology with 3.2Gbps wire-speed non-blocking Switch Fabric

System Throughput: 1.785Mpps

MAC Address: 2000

Packet Buffer: Embedded 1Mbits shared buffer

Transfer performance: 14,880pps for Ethernet and 148,810pps for Fast Ethernet

Transfer packet size: from 64 to 1536Bytes

Interface

Number of Ports:

6 x 10/100Base-TX ports

Connectors:

10/100TX: M12 D-coding 4-pin socket

Power: M12 A-codeing 5-pin connector

Cable:

10/100 Base-TX: 2-pair cable

Diagnostic LED:

Power LED: Power 1/Power 2 (Green)

Fast Ethernet Port 1~6: Link (Green)/Activity (Green blinking),

Power Requirements

Power Consumption:

Operating Voltage: 12 to 48V DC

Power consumption: max 6 Watts @ 48V

Mechanical

Protection class: IP68

Installation: Wall mount

Case: Aluminum metal case

Dimension: 213.6 mm (H) x 106.0 mm (W) x 56.5 mm (D)

Weight: 1095 g without package

Environmental

Operating Temperature: -25 ~ 70OC

Storage Temperature: -40 ~ 85OC

Regulatory Approvals

DNV: pending

EN 50155 Railway: compliance

Safety: CE/EN60950

EMI:

FCC Class A; CE/EN55022:2003 Class A;

CE/EN61000-3-2:2001 Harmonic Test;

CE/EN61000-3-3:1995 Flicker test

EMS:

EN61000-4-2:1998,ESD

EN61000-4-3:1998, RS

EN61000-4-4:1995, EFT

EN61000-4-5:1995, Surge

EN61000-4-6:1996, CS

EN61000-4-8:PFM

Shock: IEC60068-2-27

Vibration: IEC60068-2-6

Free Fall: IEC60068-2-32

B.5. JetNet 3706-RJ

Technology

Standard:

IEEE 802.3 10Base-T

IEEE 802.3u 100Base-TX

IEEE 802.3af Power Over Ethernet (PoE)

IEEE802.3x Flow control and back pressure

Broadcast storm control

Performance

Switch Technology: Store and Forward with 2.0Gbps switch fabric

System Throughput: 1.785Mpps

MAC Address: 2000

Packet Buffer: 448kbits Embedded packet buffer

Transfer performance: 14,880pps for Ethernet and 148,810 for Fast Ethernet

Transfer packet size: from 64 to 1536 Bytes

PoE Technology: End-Span wiring architecture with AC disconnection behavior Provides PD classification detection, class ID 0~3 follow IEEE802.3af standard

Pin assignment: V+ (Pin 4, 5), V- (Pin 7, 8), TX (Pin 1, 2), RX (Pin 3, 6)

Interface

Number of Ports:

4 x 10/100Base-TX Ports auto negotiation speed, F/H duplex mode, and auto MDI/MDIX connection with PoE injector

2 x 10/100Base-TX Ports auto negotiation speed, F/H duplex mode, and auto MDI/MDIX connection

Connectors:

10/100TX: Rugged RJ45 with IP67 grade protection

Redundant Power: M12 A-coded male 5 pin connector, Pin assignment (Pin1: V1+, Pin3: V-, Pin4: V2+)

LED Indicators: Power, 10/100M, Link/Acts

Power: Power 1 / Power 2 (Green)

Fast Ethernet: Link (Green) / Activity (Green blinking),

PoE: Power on (Blue)

Cable:

10Base-T: 4-pair UTP/STP Cat. 4, 5 cable,

100Base-TX: 4-pair UTP/STP Cat.5,

Cat.5E/Cat.6 cable,

Power Requirements

Power Consumption:

Operating voltage: DC 44~57V

8Watts @ 48V (Maximum) without PD loading

Mechanical

Protection class: IP67

Installation: Wall mount

Case: Aluminum metal case

Dimension: 213.6 mm (H) x 106.0 mm (W) x 56.5.0 mm (D)

Weight: 1025 g without package

Environmental

Operating Temperature: -40 ~ 70OC

Storage Temperature: -40 ~ 85OC

Regulatory Approvals

Safety: CE/EN60950(Pending)

EMI:

FCC Class A; CE/EN55022:2003 Class A

EMS:

EN61000-4-2:1998,ESD

EN61000-4-3:1998, RS

EN61000-4-4:1995, EFT

EN61000-4-5:1995, Surge

EN61000-4-6:1996, CS

EN61000-4-8:PFM

Shock: IEC60068-2-27

Vibration: IEC60068-2-6

Free Fall: IEC60068-2-32

Further Support

Korenix Technologies Co., Ltd.
9F, No. 100-1, Ming-Chuan Rd., Shing Tien City, Taipei, Taiwan
Tel: +886-2-82193000
Fax: +886-2-82193300
Business service: sales@korenix.com
Customer service: koreCARE@korenix.com